User Manual
X7968r

Broadband Wireless Gateway
ADSL2+ Bridge/Router
with integrated 802.11b/g WLAN AP
and 4-port Fast Ethernet switch

Issue 1.0
16th Jan. 2008

Table of Contents

1 Introduction 1

Features 1

Device Requirements 2

Using this Document 2

Notational conventions 2

Typographical conventions 2

Special messages 2

2 Getting to know the device 3

Parts Check 3

X7968r Front Panel 4

X7968r Rear Panel 5

3 Connecting your device 6

Connecting the Hardware 6

Step 1. Connect the DSL cable and optional telephone line 7

Step 2. Connect the Ethernet cable 7

Step 3. Attach the power connector 7

Step 4. Configure your Ethernet PCs 7

Step 5. Install a Wireless card and connect Wireless PCs 7

Next step 7

4 Getting Start with the Web pages 8

Accessing the Web pages 8

Commonly used buttons 10

Help information 11

Testing your Setup 11

Default device settings 12

5 Home 13

Overview Page 13

Basic Overview 13

Advanced Overview 14

Status – Routing Table 16

Status – DHCP Table 16

Status – Wireless Connection 16

Status – ARP Table 17

Status – Traffic Statistics 17

Trouble Shooting 18

6 Configuration 19

Quick Setup....19
Configuring ATM PVC....20
Configuring the Connection Type....20
Configuring the WAN IP Settings if PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE)....20
Configuring the WAN IP Settings if RFC1483 (Routed)....23
Configuring the WAN IP Settings if Bridging....24
Wireless Network....25
Basic Settings....25
Advanced Settings....27
WDS Settings....28
MAC Filtering....29
Registrar....29
Internet Connection Page....30
Connections....30
ADSL Configuration....31
MAC Spoofing....32
Local Network (LAN) Page....33
IP Address....33
DNS Client....34
DNS Relay....34
DNS Local Host....35
DHCP server Page....36
Global Settings....36
Server Settings....37
VLAN Configuration....39
Port - PVC Page....40
7 Security....41
IP Filtering....41
IP Filter Settings....41
Port Filters....42
IP Filters....42
Domain Filtering....43
Port Forwarding Configuration....44
Virtual Server....45
MAC Filtering....46
8 Services....47
IGMP Proxy....47
IP Routing....47
Static Routing....47
Dynamic Routing....48
Dynamic DNS....49
Quality of Service....51

Classifier *51*
QoS Setting *52*
UPnP 53
9 Port Statistics 54
DSL (A1) 54
Basic: *54*
Advanced: *55*
Wireless 56
Basic: *56*
Advanced: *57*
Raw-Ethernet 58
Basic: *58*
Advanced: *58*
Ethernet 59
Basic: *59*
Advanced: *59*
10 Admin 60
Firmware Upgrade 60
Backup & Restore 61
Reboot 62
Remote Access 63
Change Password 64
Time Zone 65
SNTP Client: *65*
SNTP Server: *66*
11 Appendix A - Configuring the Internet Settings 67
Configuring Ethernet PCs 67
Before you begin *67*
Windows Vista PCs *67*
Windows XP PCs *67*
Windows 2000 PCs *68*
Windows Me PCs *68*
Windows 95, 98 PCs *69*
Windows NT 4.0 workstations *70*
Assigning static Internet information to your PCs *70*
Configuring Wireless PCs 71
Positioning the wireless PCs *71*
Wireless PC cards and drivers *71*
Configuring PC access to your Wireless device *71*
12 Appendix C - IP Addresses, Network Masks, and Subnets 72
IP Addresses 72
Structure of an IP address *72*

Network classes *72*
Subnet masks 73
13 Appendix D - Troubleshooting 74
Troubleshooting Suggestions 74
Diagnosing Problem using IP Utilities 76
Ping *76*
nslookup *76*
14 Appendix E - Advanced DSL port attributes 78
15 Appendix F - Glossary 83
16 Appendix G - Specification 92
17 Appendix I - Regulation 94

1 Introduction

Congratulations on becoming the owner of the X7968r, ADSL router. You will now be able to access the Internet using your high-speed DSL connection.

This User Guide will show you how to connect your X7968r DSL Modem, and how to customize its configuration to get the most out of your new product.

The following specific model is covered by this user manual:
X7968r : ADSL2+, WLAN 802.11b/g AP and 4 port switch.

> **WARNING: Telefonica de España can not be held responsible for the device configuration using this manual. The present manual is sole responsibility of Amper/Xavi**

Features

The list below contains the main features of the device and may be useful to users with knowledge of networking protocols. If you are not an experienced user, the chapters throughout this guide will provide you with enough information to get the most out of your device.

The features include:

- High Speed Asymmetrical Data Transmission on Twisted Copper Pair Wire
- Service providers can deploy ADSL rapidly over existing wire infrastructure (POTS or ISDN line)
- Compatible and interoperable with most central office site ADSL DSLAM or Multi-service Access Systems.
- RFC 1483 Bridging and Routing over ATM over ADSL
- PPPoE, IPoA and PPPoA routing over ADSL
- Interchangeable between Bridge and Router mode
- Network address translation (NAT) functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Client
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- Built-in four-port 10/100BaseTX Ethernet switch for PC or LAN connection
- 802.11b/g WLAN supports up to 54Mbps
- Provides Allow/Deny Wireless MAC address list for wireless access control
- 64 and 128-bit WEP key lengths are supported
- Supports Wi-Fi WPA and WPA2 in PSK mode
- Supports 802.1Q tagged VLAN and 802.1p as well as standard compliant IP QoS for multiple services and triple play deployment.
- Configuration and management with Telnet through the Ethernet interface, and remote Telnet through ADSL interface
- Firmware upgradeable through TFTP or HTTP
- User-friendly configuration program accessed via a web browser

Device Requirements

In order to use the X7968r, you must have the following:

- DSL service up and running on your telephone line
- Instructions from your ISP on what type of Internet access you will be using, and the addresses needed to set up access
- One or more computers, each containing an Ethernet card (10Base-T/100Base-T network interface card (NIC)).
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v4 or later, or Netscape v4 or later. Note that version 4 of each browser is the minimum version requirement – for optimum display quality, use Internet Explorer v5, or Netscape v6.1

Note

You do not need to use a hub or switch in order to connect more than one Ethernet PC to the device. Instead, you can connect up to four Ethernet PCs directly to the device using the ports labeled LAN1 to LAN4 on the rear panel.

Using this Document

Notational conventions

Acronyms are defined the first time they appear in the text and also in the glossary.

For brevity, the ***X7968r*** is referred to as "the device".

The term LAN refers to a group of Ethernet-connected computers at one site.

Typographical conventions

Italic text is used for items you select from menus and drop-down lists and the names of displayed web pages.

Bold text is used for text strings that you type when prompted by the program, and to emphasize important points.

Special messages

This document uses the following icons to draw your attention to specific instructions or explanations.

Note

Provides clarifying or non-essential information on the current topic.

Definition

Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.

WARNING

Provides messages of high importance, including messages relating to personal safety or system integrity.

2 Getting to know the device

Parts Check

In addition to this document, your package should arrive containing the following:

- ***The device (X7968r)***
- ***Ethernet cable***
- ***Standard phone/DSL line cable***
- ***Power adapter***
- ***User Manual CD***

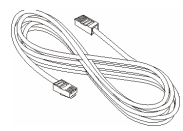
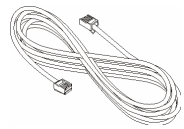
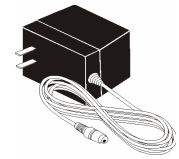
	X7968r ADSL device unit
	RJ-45 Cable
	RJ-11 Cable
	Power adapter
	User's Manual CD

Figure 1: DSL Modem Package Contents

X7968r Front Panel

The front panel contains lights called Light Emitting Diodes (LEDs) that indicate the status of the unit.

Figure 2: Front Panel and LEDs

Label	Color	Function
Ethernet	Green	On: LAN link established and active Off: No LAN link Blink: Data being transmitted
WLAN	Green	On: Wireless function enabled Off: Wireless function disabled Blink: Data being transmitted
⏻	Green	On: device is powered on Off: device is powered off
ADSL	Green	On: DSL link reaches showtime, which means that your device has successfully connected to your ISP's DSL network. Off: DSL link not in showtime, your device has not successfully connected to your ISP's DSL network. Slow blink: Try to connect to ISP's DSL network
PPP	Green	On: There is a PPPoA or PPPoE connection. Off: There is no PPPoA or PPPoE connection. Blink: There is traffic on PPP connection

IMPORTANT: A simultaneous rithmic blink of ADSL and PPP LEDs means that flash memory is being writen. Router shouldn't be unpowered in this state!

X7968r Rear Panel

The X7968r rear panel contains the ports for the unit's data and power connections.

Figure 3: Rear Panel Connections

Label	Function
ON / OFF	ON/OFF switch
12V-1A	Connects to the supplied power adapter
1X ~ 4X Ethernet	Connects the device via Ethernet to your devices in LAN
(( ))	Press and hold this button for 1 second to enable Wireless AP function or disable it
RESET	A reset button to reset the device or reset to default settings. Press and hold for 5 seconds.
ADSL	Connects to the ISP DSL network

3 Connecting your device

This chapter provides basic instructions for connecting the device to a computer or LAN and to the Internet.

In addition to configuring the device, you need to configure the Internet properties of your computer(s). For more details, see the following sections in Appendix A:

Configuring Ethernet PCs section

Configuring Wireless PCs section

This chapter assumes that you have already established a DSL service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Connecting the Hardware

This section describes how to connect the device to the power outlet and your computer(s) or network.

WARNING

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and the device.*

The diagram below illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

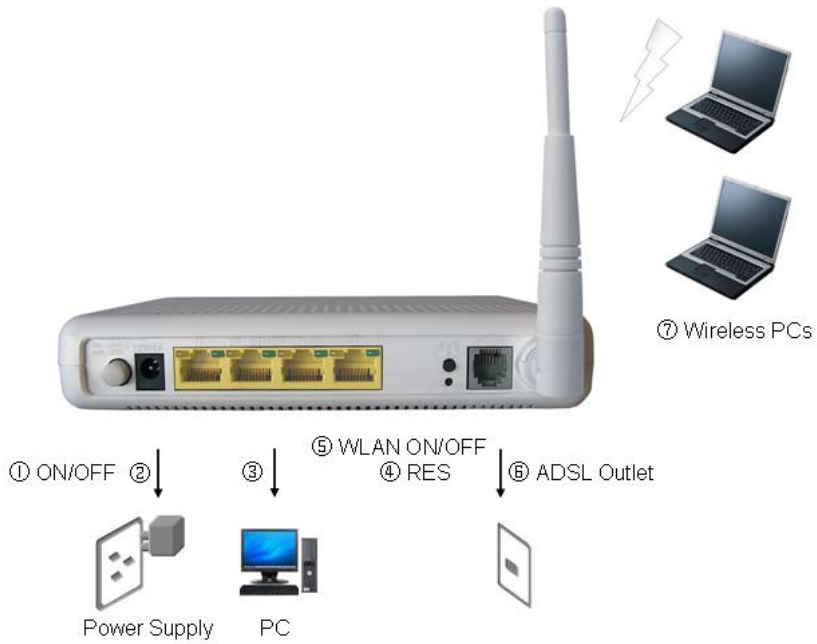


Figure 4: Overview of Hardware Connections for X7968r

Step 1. Connect the DSL cable and optional telephone line

Connect one end of the provided phone cable to the port labeled DSL on the rear panel of the device. Connect the other end to ADSL spliter.

Step 2. Connect the Ethernet cable

Connect up to four single Ethernet computers or to a HUB/Switch directly to the device via Ethernet cable(s).

Note that the cables do not need to be crossover cables.

Step 3. Attach the power connector

Connect the AC power adapter to the Power connector on the back of the device and plug the adapter into a wall outlet or power strip. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 4. Configure your Ethernet PCs

You must also configure the Internet properties on your Ethernet PCs. See Configuring Ethernet PCs section.

Step 5. Install a Wireless card and connect Wireless PCs

You can attach a Wireless LAN that enables Wireless PCs to access the Internet via the device.

You must configure your Wireless computer(s) in order to access your device. For complete instructions, see Configuring Wireless PCs section.

Next step

After setting up and configuring the device and PCs, you can log on to the device by following the instructions in "Getting Started with the Web pages" on chapter 4. The chapter includes a section called Testing your Setup, which enables you to verify that the device is working properly.

4 Getting Start with the Web pages

The DSL Modem includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through a web browser on a PC connected to the device.

Accessing the Web pages

To access the web pages, you need the following:

A laptop or PC connected to the LAN or WLAN port on the device.

A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox from any of the LAN computers, launch your web browser, type the URL, **http://192.168.1.1** in the web address (or location) box, and press [Enter]. Then enter the default username and password: admin/admin to access the configuration web page, if you have not changed the username and password.

The home page opens displaying the overview of device:

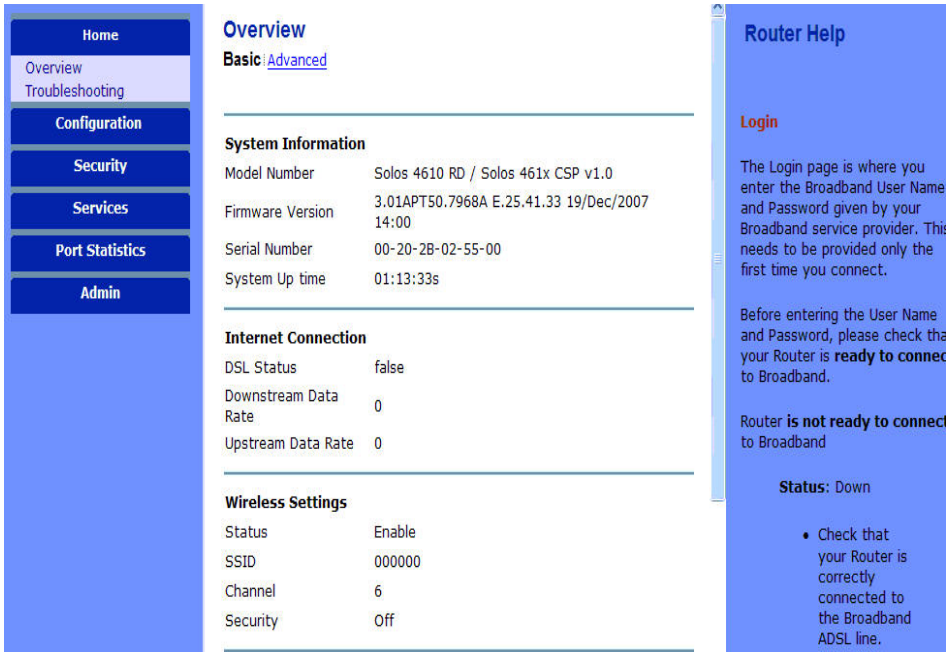


Figure 5: Overview –Home

The Menu comprises:

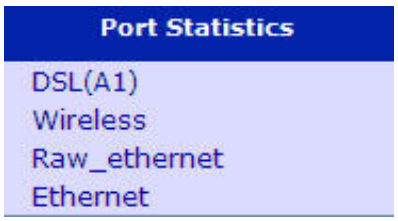
***Home (My DSL Modem)*:** provides overview and troubleshooting of the system. It includes the sub menus Overview and Troubleshooting. By default, the page Overview is displayed after the login.

Configuration: provides information about the current configuration of various system features with options to change the configuration. It includes the sub menus Quick Setup, Wireless Network, Internet Connection, Local Network, DHCP Server, VLAN Config and Port-PVC.

Security: provides filtering, forwarding, and setting up the virtual server. It includes the sub menus IP Filtering, Domain Filtering, Port Filtering, Virtual Server, and MAC Filtering.

Service: provides services such as IGMP Proxy (enabling the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces), IP Routing, Dynamic DNS, Qualify of Service and UPnP.

Port Statistics: Let you view the values of port parameters (DSL, Wireless, Raw_ethernet, and Ethernet).



Admin: provides the administration utilities such as firmware upgrade, backup & restore, reboot, remote access, change password and Time Zone.

Commonly used buttons

The following buttons are used throughout the web pages:

Button	Function
Next >	You may need to configure the default settings on more than one Web page. Click on this button once you have changed the configuration on your current page and are ready to move on to the next.
Cancel	This button appears on every configuration page. Click on this button if at any time you decide that you do not want to change the existing settings.
Disabled Enabled	Radio buttons – these appear on many configuration pages. You will be asked to select one radio button from the selection of two or more available. You cannot select more than one radio button at a time.
Apply	This button appears on every configuration page. Click on this button once you are through with the changes and decide to apply the made changes.
Browse...	You may need to browse to find a file which needs to be uploaded for new configuration.
Upgrade	This button allows you to upgrade to the new configuration file attached using the Browse button.

The following terms are used throughout this guide in association with these buttons:

Click – point the mouse arrow over the button, menu entry or link on the screen and click the left mouse button. This performs an action, such as displaying a new page or performing the action specific to the button on which left mouse button is clicked.

Select – usually used when describing which radio button to select from a list, or which entry to select from a drop-down list. Point the mouse arrow over the entry and left-click to select it.

This does not perform an action – you will also be required to click on a button, menu entry or link in order to proceed.

Help information

To view the help, click the desired menu or submenu. The related help information appears in the right pane.

Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the device's DSL connection to access the Internet.

To test the connection, turn on the device, wait for 30 seconds and then verify that the LEDs are illuminated as follows:

LED	Behavior
Encendido	Solid green to indicate that the device is turned on. If this light is not on, check the power cable attachment.
WLAN	Solid green to indicate that the Wireless LAN function is operational.
LAN	Solid green to indicate that the device can communicate with your LAN.
ADSL	Flashing on/off while trying to SYNC UP with ISP CO site. Solid green to indicate that the device has successfully established a connection with your ISP.
PPP	On: There is a PPPoA or PPPoE connection. Off: There is no PPPoA or PPPoE connection.

Table 1. LED Indicators

If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website (such as *http://www.yahoo.com*).

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. If the LEDs still do not illuminate as expected or the web page is not displayed, see Troubleshooting section or contact your ISP for assistance.

Default device settings

In addition to handling the DSL connection to your ISP, the DSL Modem can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

WARNING

We strongly recommend that you contact your ISP prior to changing the default configuration.

Option	Default Setting	Explanation/Instructions
User/Password	admin/admin	User name and password to access the device
DSL Port IP Address	Unnumbered interface: 192.168.1.1 Subnet mask: 255.255.255.255	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. See *Quick Setup* section.
LAN Port IP Address	Assigned static IP address: 192.168.1.1 Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See *Local Network* section.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.2 through 192.168.1.21 (Please be noted that the default DHCP IP address pool may be different in each firmware version.)	The device maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in *DHCP Server* section.

5 Home

The Home web page menu includes the following submenus:

Overview
Trouble Shooting

Overview Page

The overview of the device contains most of the basic information like

System Information (equipment vendor, model number, chipset part number, chipset version number),

Internet Information (ADSL port, downstream rate, upstream rate, default Gateway, Primary DNS Server, Secondary DNS server),

Wireless Setting Information (Status, SSID, Channel, Security),

LAN Port information (MAC address, IP address, Subnet Mask and DHCP server).

Basic Overview

Figure 6: Overview – Basic

Advanced Overview

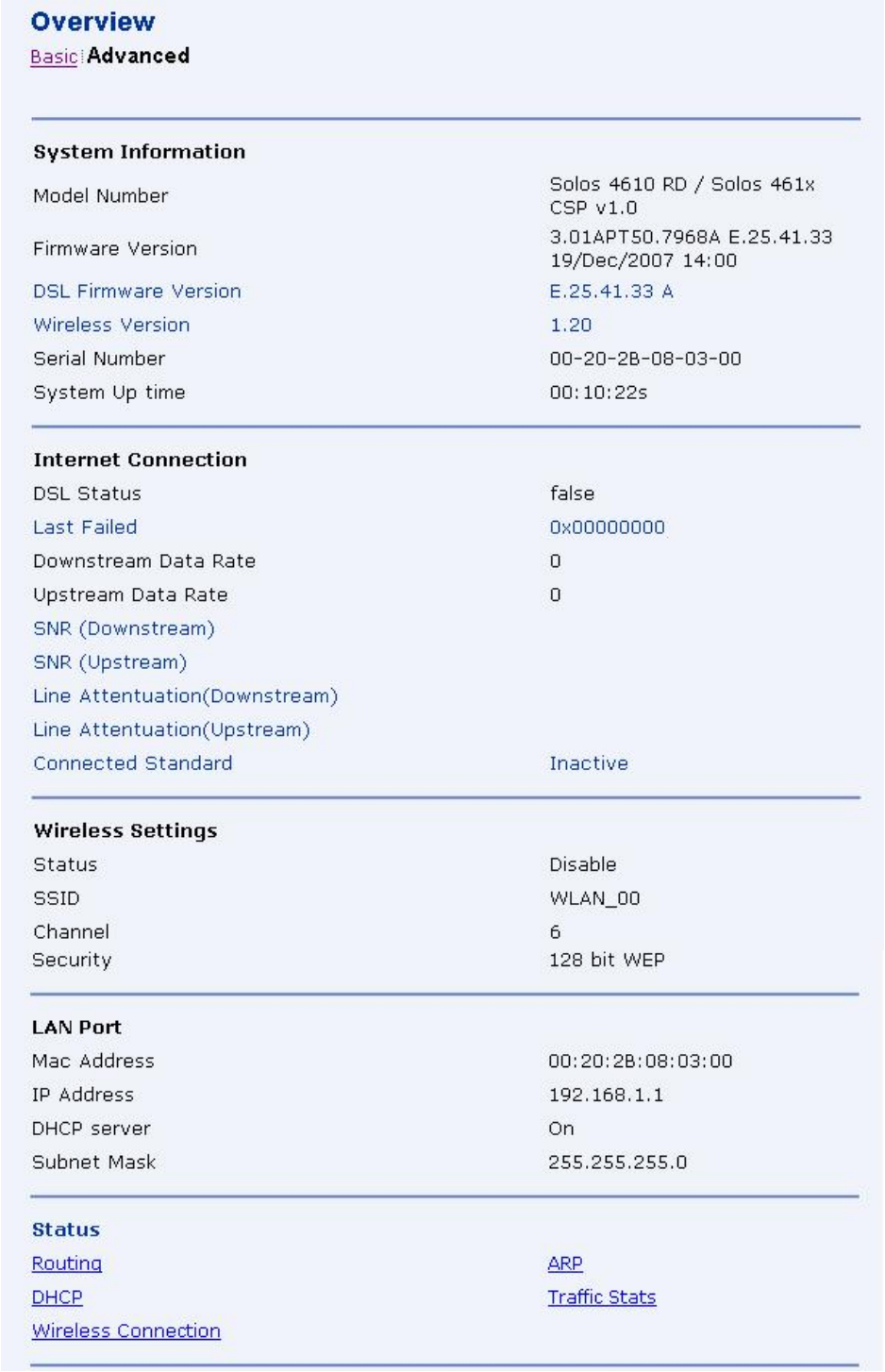


Figure 7: Overview – Advanced

The Advanced information of the device includes the following:

- System Information – In addition to the information displayed as under *Basic*, it also displays the *DSL Firmware Version* and *Wireless Version*.
- Internet Connection – In addition to the information displayed as under Basic, it also displays Last Failed internet connection, SNR (Downstream), SNR (Upstream), Line Attenuation (Downstream), Line Attenuation (Upstream), and the Connected Standard.

- Wireless Settings - displays the wireless settings for the modem.
- LAN Port – displays the same information as displayed under *Basic*.
- Status – displays the status of *Routing*, *DHCP*, *ARP*, *Wireless Connection*, and *Traffic*.

Status – Routing Table

This web page shows the routing table of the device which shows the packet flow when the device receives incoming packets from WAN port and LAN port.

Figure 8: Routing Table

Status – DHCP Table

This web page shows all the PCs who request an IP address from the device. Those messages show in the web page, MAC address of PC, assigned IP address, Lease Time and the host name of PC.

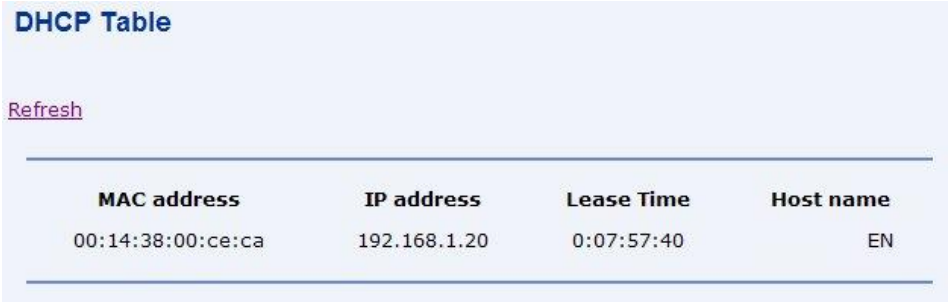


Figure 9: DHCP Table

Status – Wireless Connection

This web page shows current connected Wireless PCs.

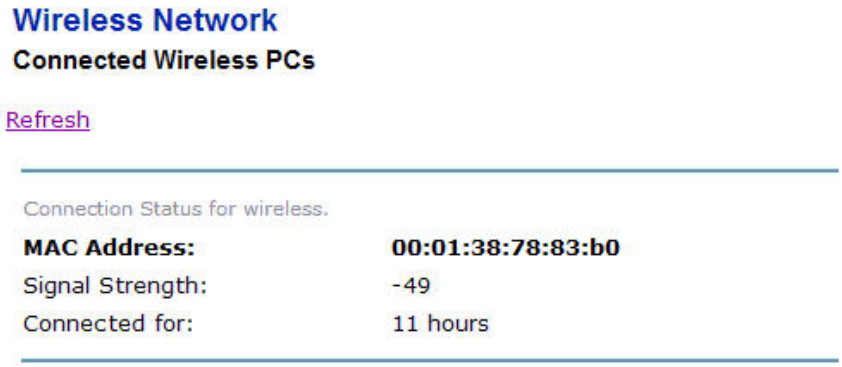


Figure 10: Status of Connected Wireless PCs

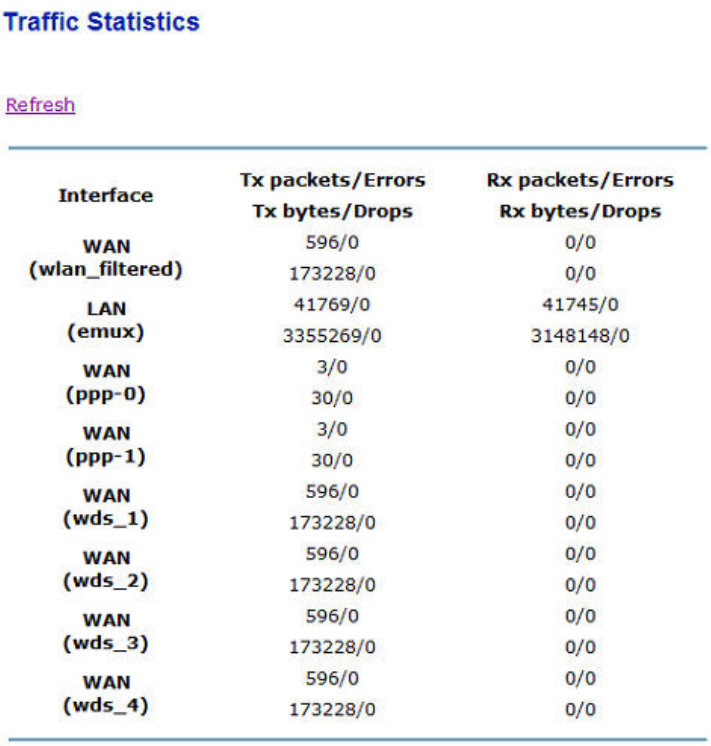
Status – ARP Table

This web page shows the relationship between MAC address and IP address where the device learns from the data traffic. Besides, it also records the interface where the device learns this information.

Figure 11: ARP Table

Status – Traffic Statistics

This web page shows traffic statistics of TX&RX both directions including wireless port, four Ethernet ports, HPNA port and WAN ports.



Interface	Tx packets/Errors Tx bytes/Drops	Rx packets/Errors Rx bytes/Drops
WAN (wlan_filtered)	596/0 173228/0	0/0 0/0
LAN (emux)	41769/0 3355269/0	41745/0 3148148/0
WAN (ppp-0)	3/0 30/0	0/0 0/0
WAN (ppp-1)	3/0 30/0	0/0 0/0
WAN (wds_1)	596/0 173228/0	0/0 0/0
WAN (wds_2)	596/0 173228/0	0/0 0/0
WAN (wds_3)	596/0 173228/0	0/0 0/0
WAN (wds_4)	596/0 173228/0	0/0 0/0

Figure 12: Traffic Statistics

Trouble Shooting

This page provides you an option to troubleshoot (ping websites and run diagnostic tests) in case of some error.

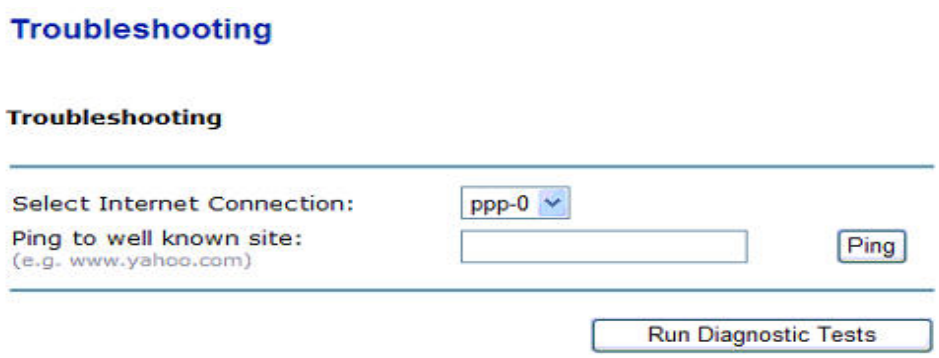
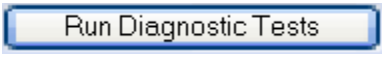


Figure 13: Trouble Shooting

- Select the type of internet connection from Select Internet Connection drop down menu. The internet connections currently valid for your device are displayed in the drop down list. For example pppoa, pppoe, or Rfc1483Up.
- Enter the well known site in Internet and click Ping to check the path between the device and web site is OK or not.
- Click on 

to run the diagnostic test on the internet connection. For example, you may get diagnostic information as displayed in the following screenshot. In this case, the ADSL connection is failed that you have to check the ADSL line is well connected and installed before you go for next step.

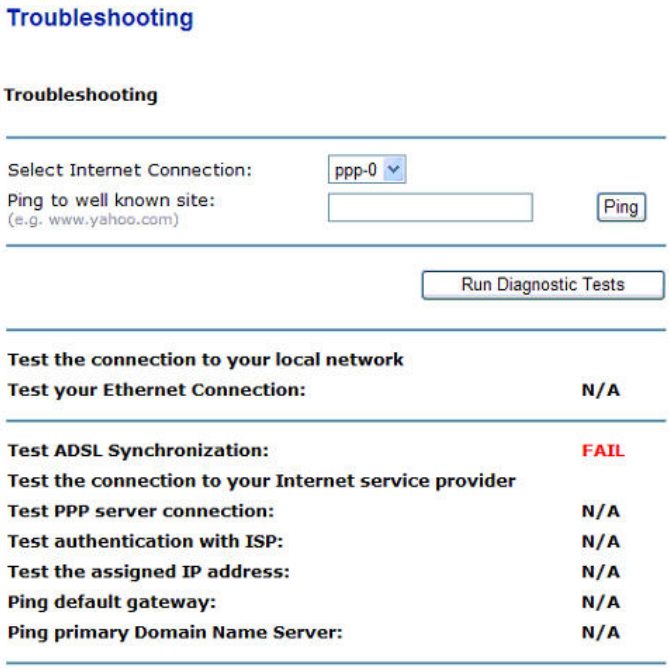


Figure 14: Trouble Shooting – Running Diagnostic Tests

6 Configuration

The Configuration web page menu comprises:

Quick Setup
Wireless Network
Internet Connection
Local Network (LAN)
DHCP Server
VLAN Config
Port-PVC

Quick Setup

The Quick Setup page available under Configuration menu option is required to setup your device if it is not yet connected to internet. Before accessing quick setup, you should ask for the following information from your ISP:

- VPI/VCI
- Protocol: PPPoA, PPPoE, IPoA, RFC1483 (Routed), or Bridging
- Encapsulation Type: VCMUX or LLC/SNAP
- IP settings: Dynamic or Fixed. If fixed, then your ISP should also provide you an IP address
- NAT: Disabled or Enabled
- Add Default Route: Disabled or Enabled
- PPP User Name and Password (also known as Broadband User Name and Password)

To display quick setup page:

- Click Quick Setup under Configuration.

Configure ATM PVC page opens:

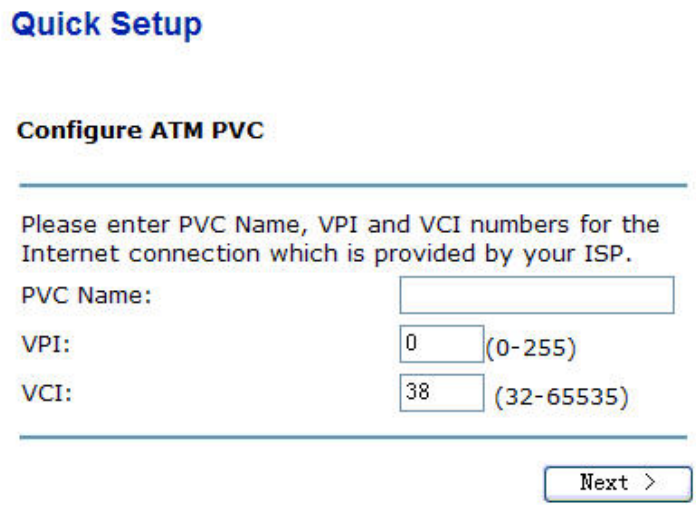


Figure 15: Quick Setup

The information displayed on this page and the pages that follow are explained in detail in the following sub sections.

Configuring ATM PVC

To configure ATM PVC:

- Enter the PVC Name such as the name of ISP
- Configure the ATM PVC by entering the VPI and VCI values provided by the ISP.
- Click Next.

Configuring the Connection Type

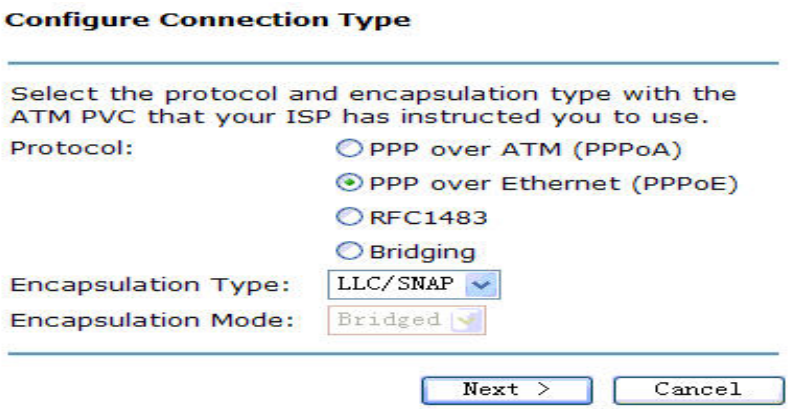


Figure 16: Configuring the Connection Type

To configure the connection type:

- Select the Protocol by selecting the radio button for the desired protocol type.
- Select the Encapsulation Type from the drop down list (VCMUX or LLC/SNAP).
- Select the Encapsulation Mode from the drop down list (Bridged or Rotued).

Configuring the WAN IP Settings if PPP over ATM (PPPoA) or PPP over Ethernet (PPPoE)

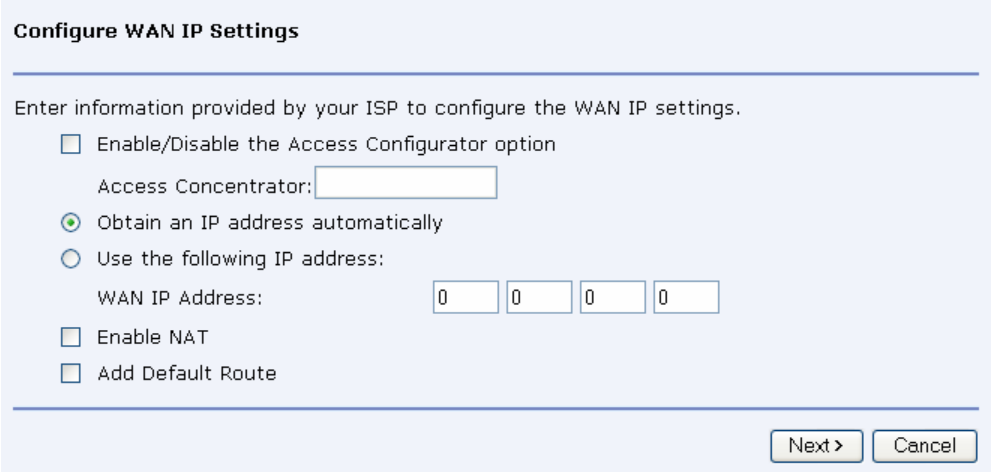


Figure 17: Configuring WAN IP Settings

To configure the WAN IP settings:

- Select/Unselect to enable or disable the Access Configurator option. In case, you enable the access configurator, enter the value in Access Concentrator.
- Select one of the following options:
  - Obtain an IP address automatically.
  - Use the following IP address: specify the WAN IP Address.
- Click to Enable NAT.
- Click to Add Default Route
- Click Next.

Configuring the Broadband User Name and Password

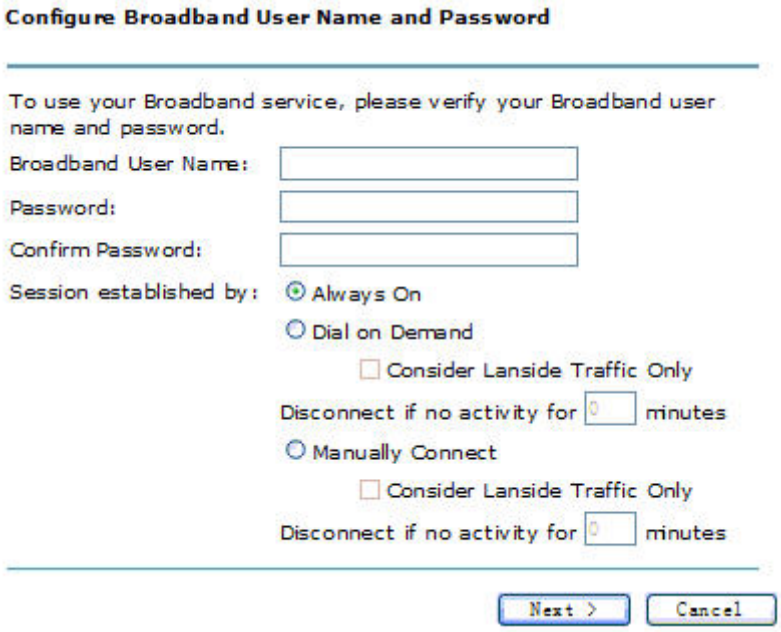

Configure Broadband User Name and Password
To use your Broadband service, please verify your Broadband user name and password.
Broadband User Name:
Password:
Confirm Password:
Session established by:
Always On
Dial on Demand
Consider Lanside Traffic Only
Disconnect if no activity for 0 minutes
Manually Connect
Consider Lanside Traffic Only
Disconnect if no activity for 0 minutes
Next >
Cancel

Figure 18: Configuring Broadband User Name and Password

To configure the broadband user name and password:

- Enter the user name in *Broadband User Name*.
- Enter the password in *Password* and confirm it by entering again in *Confirm Password*.
- Specify the network session by selecting *Always On*, *Dial on Demand* or *Manually Connect* option. You could check the *Consider Lanside Traffic Only* to specify the data traffic for *Dial on Demand* and *Manually Connect*. You can also opt to disconnect after a specified period when no user activity is detected. By default, the option *Always On* is selected.
- Click *Next*.

Configure LAN side settings

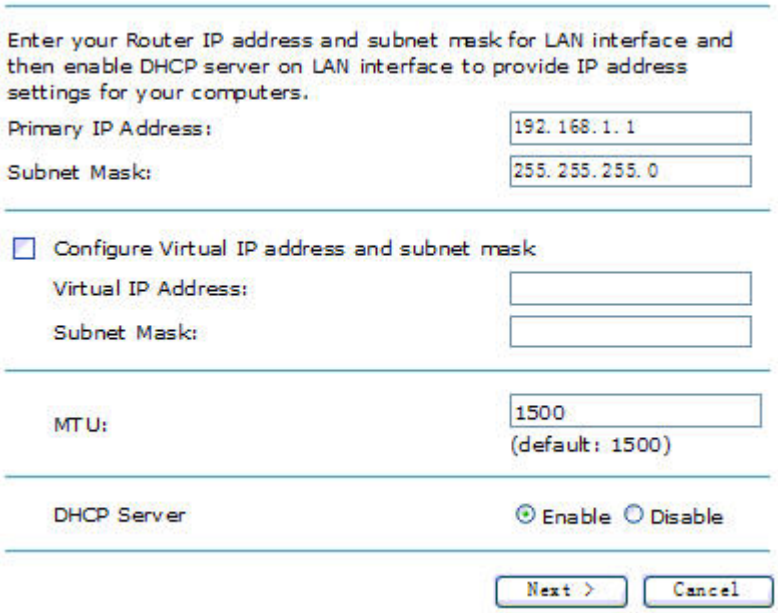


Figure 19: Configuring LAN

To configure LAN:

- Enter the primary IP address. For example, enter 192.168.1.1
- Enter the subnet mask. For example, enter 255.255.255.0
- You have the option to set up the secondary IP address. Enter the IP address and subnet mask in *Secondary IP Address* and *Subnet Mask* respectively.
- Enter the value of MTU. The default value is 1500.
- Select on one of the option: *DHCP Server Enable* or *DHCP Server Disable*.
- Click *Next*.

The following page opens to confirm the settings:

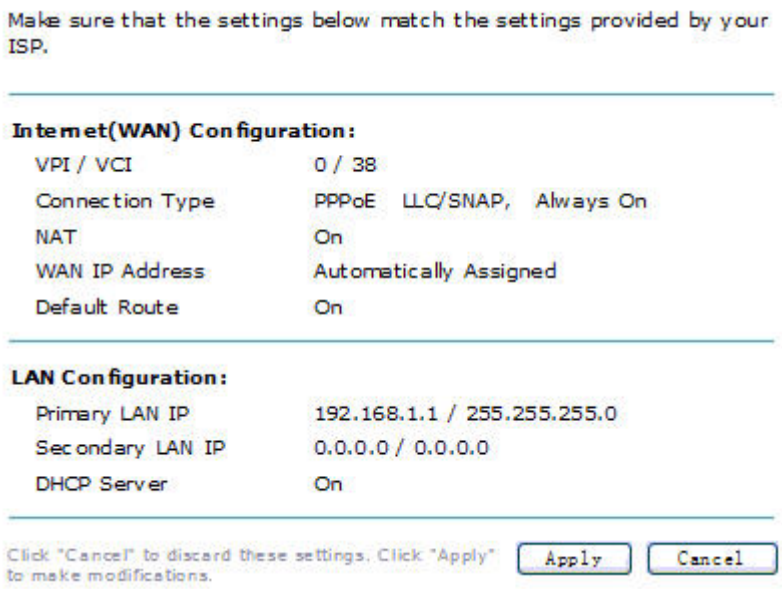

Make sure that the settings below match the settings provided by your ISP.
Internet(WAN) Configuration:
VPI / VCI 0 / 38
Connection Type PPPoE LLC/SNAP, Always On
NAT On
WAN IP Address Automatically Assigned
Default Route On
LAN Configuration:
Primary LAN IP 192.168.1.1 / 255.255.255.0
Secondary LAN IP 0.0.0.0 / 0.0.0.0
DHCP Server On
Click "Cancel" to discard these settings. Click "Apply" to make modifications.
Apply
Cancel

Figure 20: Configuring LAN - Confirm Settings

A summary of the WAN and LAN configuration is displayed. Click Apply to make the changes else click Cancel to discard the changes.

Configuring the WAN IP Settings if RFC1483 (Routed)

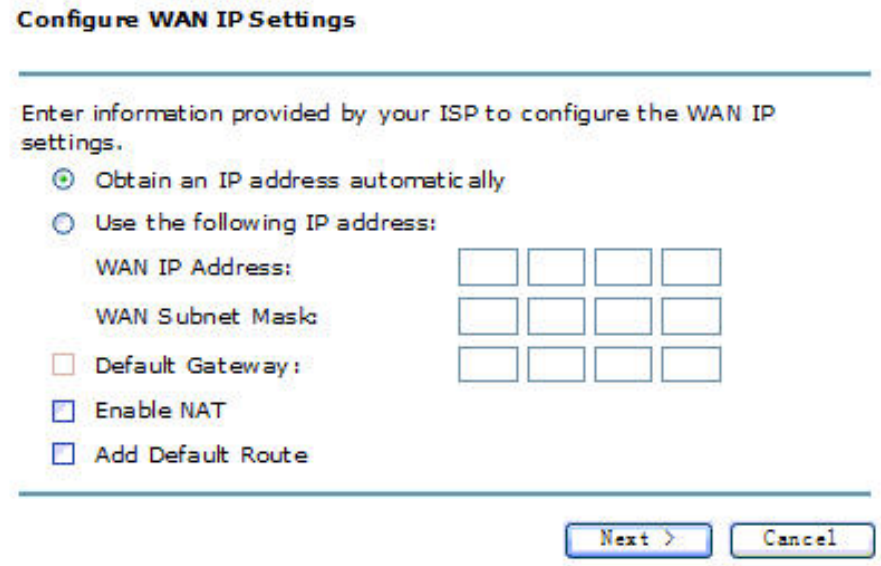


Figure 21: Configuring WAN IP Settings

To Configure WAN IP settings,

- select one of the following options:
  - Obtain an IP address automatically.
  - Use the following IP address: specify the *WAN IP Address and subnet mask*.
- Check to set Default Gateway and enter IP address of gateway if you set the WAN IP and subnet mask manually
- Click to Enable NAT.

- Check to enable Add Default Route. It means this PVC is the path of default route.
- Click *Next*.

The same procedure as configuring PPPoA or PPPoE, the configuring the LAN site settings and confirming setting pages will be shown, please follow up above descriptions to finish the settings.

Configuring the WAN IP Settings if Bridging

In this mode, the device is a bridge and passes all raw data traffic between WAN and LAN ports. There is no need for any settings.

The same procedure as configuring PPPoA or PPPoE, the configuring the LAN site settings and confirming setting pages will be shown, please follow up above descriptions to finish the settings. But be noted, the IP addresses in the PC of LAN side are visible to the WAN site in the bridging mode, those IP addresses are not blocked by NAT feature.

Wireless Network

This page allows you to setup the wireless connection. The following are the types of settings allowed:

Basic Settings
Advanced Settings
WDS Settings
MAC Address Filter
Registrar

Basic Settings

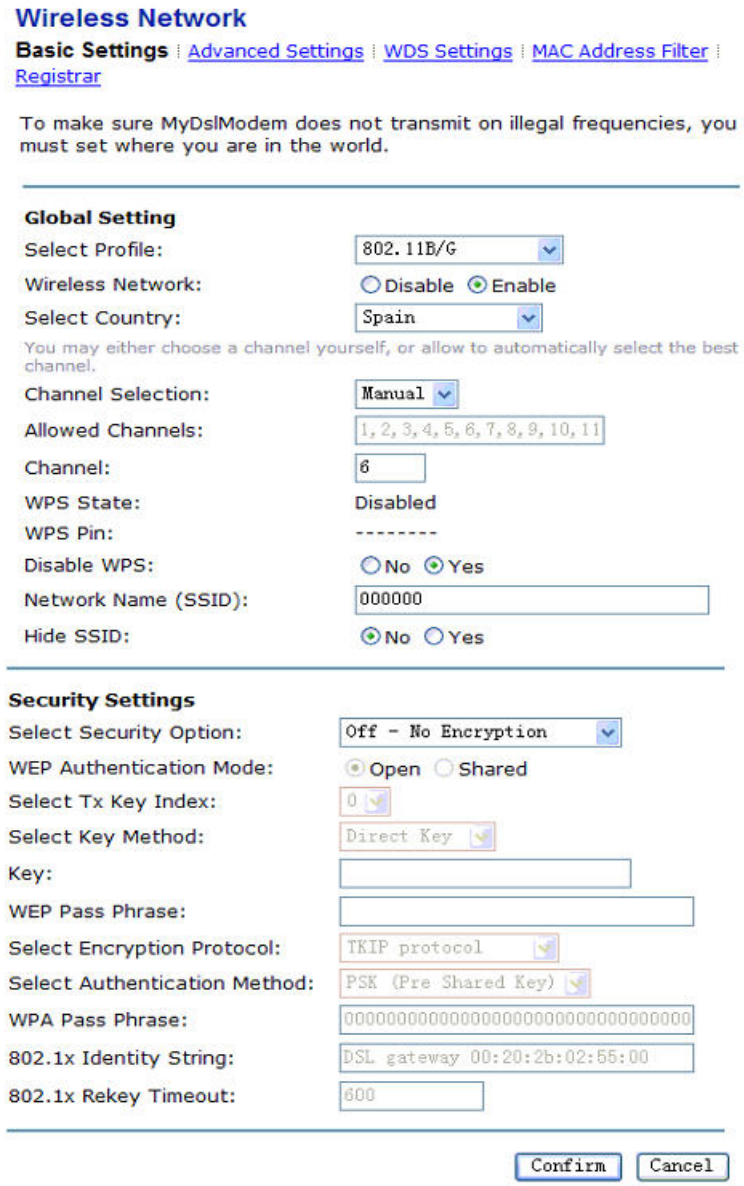

Wireless Network
Basic Settings | Advanced Settings | WDS Settings | MAC Address Filter | Registrar
To make sure MyDslModem does not transmit on illegal frequencies, you must set where you are in the world.
Global Setting
Select Profile: 802.11B/G
Wireless Network: Disable Enable
Select Country: Spain
You may either choose a channel yourself, or allow to automatically select the best channel.
Channel Selection: Manual
Allowed Channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Channel: 6
WPS State: Disabled
WPS Pin: --------
Disable WPS: No Yes
Network Name (SSID): 000000
Hide SSID: No Yes
Security Settings
Select Security Option: Off - No Encryption
WEP Authentication Mode: Open Shared
Select Tx Key Index: 0
Select Key Method: Direct Key
Key:
WEP Pass Phrase:
Select Encryption Protocol: TKIP protocol
Select Authentication Method: PSK (Pre Shared Key)
WPA Pass Phrase:
802.1x Identity String: DSL gateway 00:20:2b:02:55:00
802.1x Rekey Timeout: 600
Confirm
Cancel

Figure 22: Wireless Network – Basic Settings

Global Setting

- Select the wireless profile: 802.11b/g, 11b only, 11g only, or mixed_long.

- Enable/Disable the Wireless network.
- Select Country where you are located.
- Select the wireless communication channel by AUTO or MANUAL. If manual selection, enter the channel you wish the wireless network to use.
- Show up the current Wireless Provisioning Service (WPS) status and Pin
- Enable/Disable the WPS feature. The WPS feature enables discovery of and connection to the wireless network. It makes wireless client to connect wireless AP simple.
- Specify the Network Name (SSID) used among the device and the wireless clients.
- You may choose to Hide SSID (Yes/No). The SSID will not be broadcasted to wireless clients if you select to hide it.

Security Settings

- Select the one of security options: OFF, WEP 64bits, WEP 128bits, WPA, WPA2, WPA mixed mode.
- Select the Authentication Mode: Open or Shared
- Select TX key index: if you select the 64bits or 128bits as your wireless security method, there are 4 keys can be used. You could specify the one for usage.
- Select Key Method: you could select Direct_Key to enter the key in the KEY field or Pass Phrase to generate the key automatically. Enter the strings in the WEP Pass Phrase field if you select the Pass Phrase as your Key Method.
- Select Encryption Protocol (TKIP or AES – CCMP) if you select the WPA and WPA2.
- Specify Authentication Method, PSK (pre-share key) or EAP.
- Enter the key in the WPA Pass Phrase field if you select PSK.
- Enter 802.1x Identify String and 802.1x Rekey Timeout if you select EAP.
- Click Confirm to save the configuration.

Advanced Settings

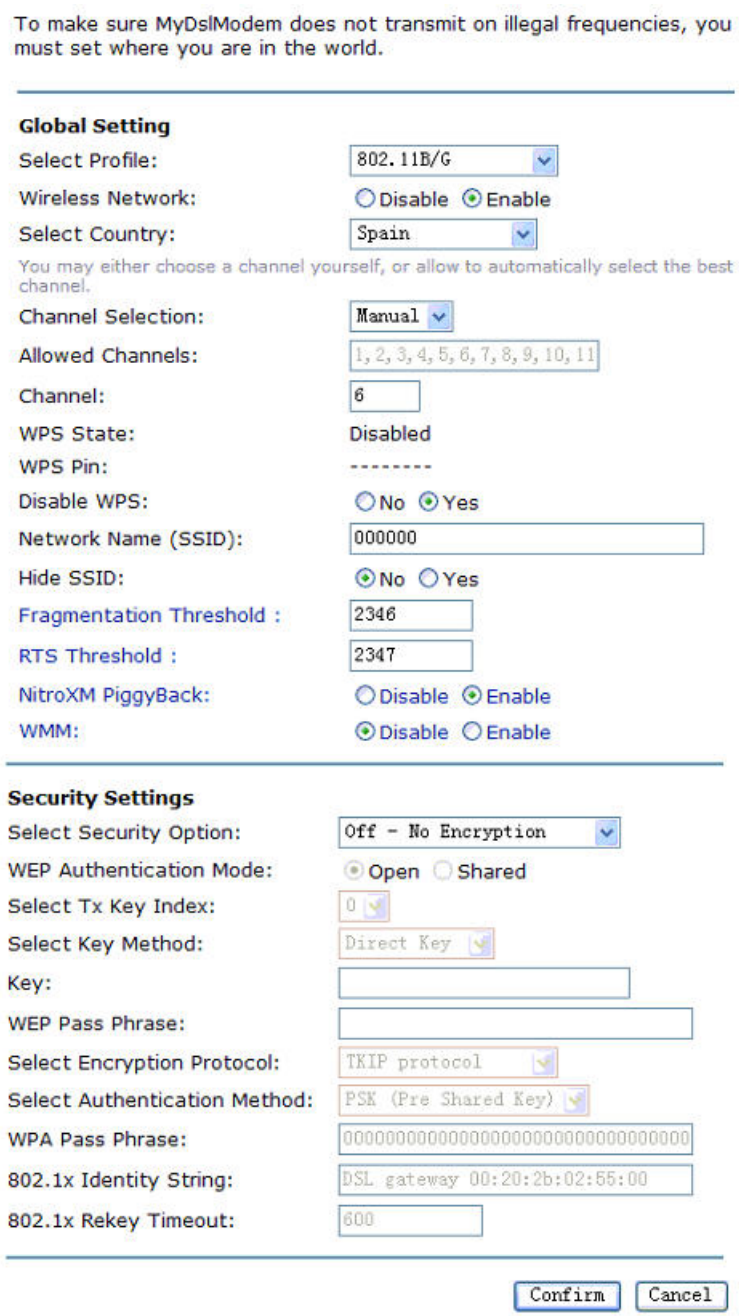

To make sure MyDslModem does not transmit on illegal frequencies, you must set where you are in the world.
Global Setting
Select Profile: 802.11B/G
Wireless Network: Disable Enable
Select Country: Spain
You may either choose a channel yourself, or allow to automatically select the best channel.
Channel Selection: Manual
Allowed Channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Channel: 6
WPS State: Disabled
WPS Pin: --------
Disable WPS: No Yes
Network Name (SSID): 000000
Hide SSID: No Yes
Fragmentation Threshold : 2346
RTS Threshold : 2347
NitroXM PiggyBack: Disable Enable
WMM: Disable Enable
Security Settings
Select Security Option: Off - No Encryption
WEP Authentication Mode: Open Shared
Select Tx Key Index: 0
Select Key Method: Direct Key
Key:
WEP Pass Phrase:
Select Encryption Protocol: TKIP protocol
Select Authentication Method: PSK (Pre Shared Key)
WPA Pass Phrase:
802.1x Identity String: DSL gateway 00:20:2b:02:55:00
802.1x Rekey Timeout: 600
Confirm
Cancel

Figure 23: Wireless Network – Advanced Settings

Global Setting

In addition to the settings provided under basic settings, you can specify Fragmentation Threshold, RTS Threshold, NitroXM PiggyBack and WMM.

Security Settings

The advanced security settings are same as provided under the basic settings.

WDS Settings

WDS stands for Wireless Distribution System. It enables the access points (AP) to be connected on wireless in the same channel to extend the coverage. You can either remove an existing WDS functionality. To remove a WDS link to an AP, reset the MAC address associated with the required port to 00:00:00:00:00:00 from web page.

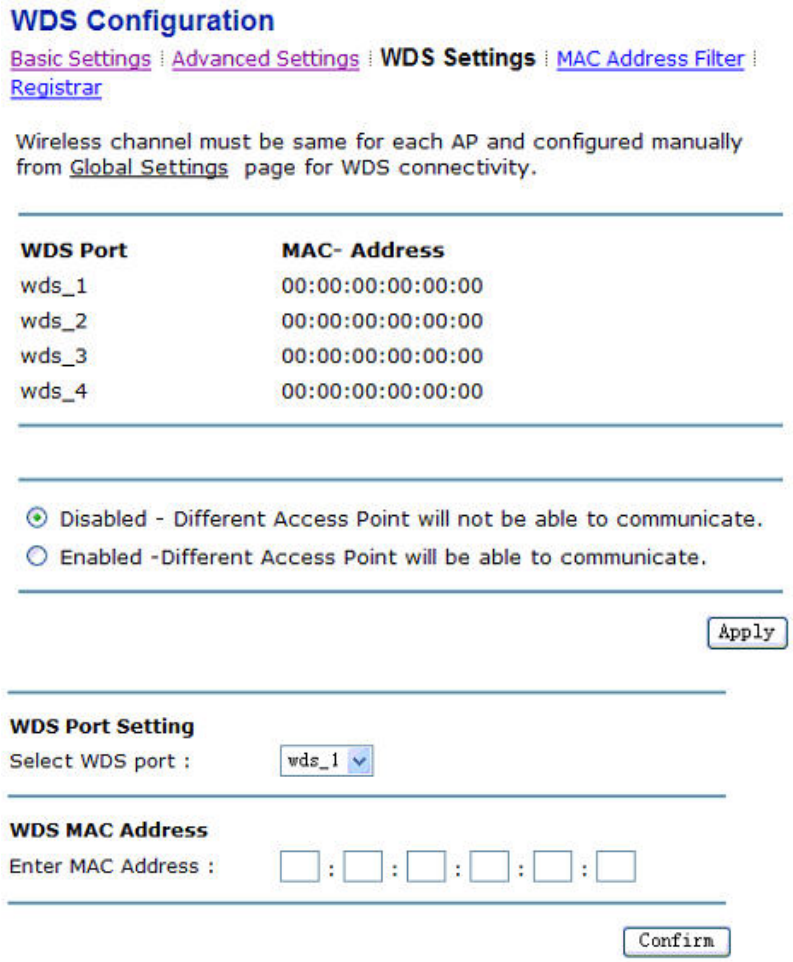

WDS Configuration
Basic Settings | Advanced Settings | WDS Settings | MAC Address Filter | Registrar
Wireless channel must be same for each AP and configured manually from Global Settings page for WDS connectivity.
WDS Port
MAC- Address
wds_1 00:00:00:00:00:00
wds_2 00:00:00:00:00:00
wds_3 00:00:00:00:00:00
wds_4 00:00:00:00:00:00
Disabled - Different Access Point will not be able to communicate.
Enabled -Different Access Point will be able to communicate.
Apply
WDS Port Setting
Select WDS port :
wds_1
WDS MAC Address
Enter MAC Address :
Confirm

Figure 24: Wireless Network – WDS Settings

Global Setting

- Enable/Disable the *Wireless Distribution System* (WDS) feature
- Click *Apply* to enable this feature.
- Select *WDS Port Setting* from 1 to 4 and enter the *MAC address* of wireless AP. To remove the WDS to an AP, just enter the 00:00:00:00:00:00 in the MAC address field to reset it.
- Click *Confirm* to add this wireless AP.

MAC Filtering

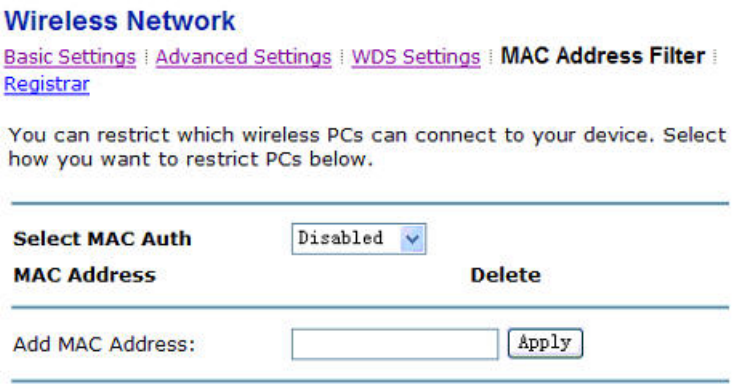

Wireless Network
Basic Settings | Advanced Settings | WDS Settings | MAC Address Filter |
Registrar
You can restrict which wireless PCs can connect to your device. Select how you want to restrict PCs below.
Select MAC Auth
Disabled
MAC Address
Delete
Add MAC Address:
Apply

Figure 25: MAC Filtering Configuration

You can specify which wireless PCs can connect or can not connect to your device.

To setup the MAC filtering feature:

- Select the *MAC Auth* method from Disable (MAC filtering feature is disabled), White List (allow those PCs to connect) or Black List (deny those PCs to connect).
- Enter the MAC address and click *Apply*. You can also delete the existing MAC address by clicking the *Delete*.

Registrar

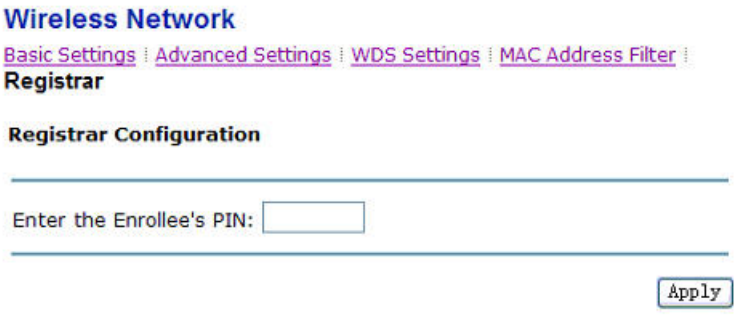


Figure 26: Wireless Network - Registrar Configuration

To access the registrar:

- Enter the *Enrollee's PIN* and click *Apply*.

Internet Connection Page

You can configure your internet connection from this page. This page displays the details of existing internet connection, if any. You can perform the following functions from this page:

Configure internet connection

Configure ADSL

Specify MAC Spoofing

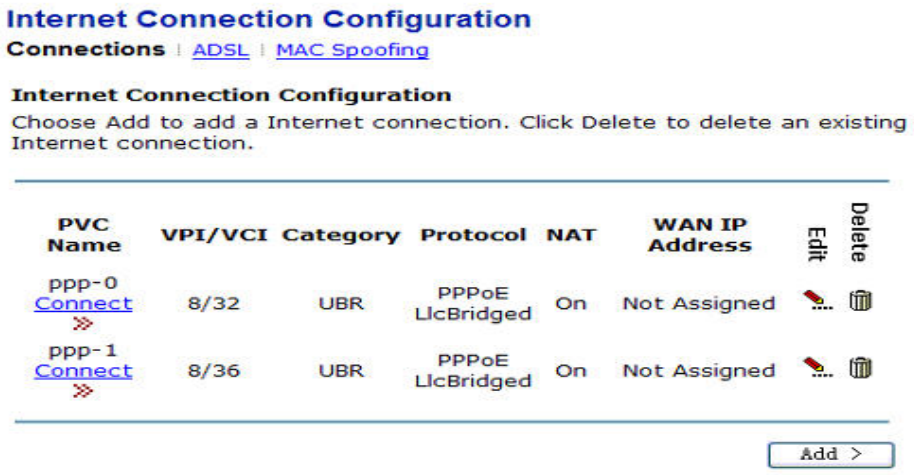


Figure 27: Internet Connection Configuration

Connections

To configure the internet connection:

- *Click Add.* Follow the steps described under Quick Setup section to setup the internet connection. If there is existing Internet connection, you may use the *Edit* or *Delete* to edit the connection profile or delete it.

ADSL Configuration

In this web page, you can configure the basic ADSL parameters like enable/disable ADSL port, ADSL mode and some specific values.

Figure 28: ADSL Configuration

To configure ADSL:

- Check the desired line modes, AnnexA, T1413A, A2Plus (ADSL2+), A2 (ADSL2), M2Plus (ADSL2+ AnnexM), M2 (ADSL2 AnnexM).
- Click Apply to save the settings.
- Click Start to take effect the settings
- Click Defaults to restore factory default settings.
- There are more detailed parameters will be shown after you click Basic Attributes, AnnexA Attributes, BisA Attributes, or BisM Attributes. If you like to get more details, please contact technician for support.

MAC Spoofing

Internet Connection Configuration
Connections | ADSL | MAC Spoofing
MAC spoofing lets MyHomeRouter identify itself as another computer or device. You may need to use this depending on your Internet Service Provider.
Select whether you need MAC spoofing enabled from the options below:
Disabled - MAC Spoofing is not used
Enabled - MAC Spoofing will be used with a MAC address you provide
Next
Cancel

Figure 29: MAC Spoofing

MAC spoofing lets the MyDslModem identify itself as another computer or device. You may need to use this depending on your Internet Service Provider.

To specify MAC Spoofing:

- Select either Disabled - MAC Spoofing is not used or Enabled - MAC Spoofing will be used with a MAC address you provide. MAC Spoofing Setup/Confirm page opens based on the option you selected earlier.
- Specify the MAC address in case you enabled the MAC Spoofing.

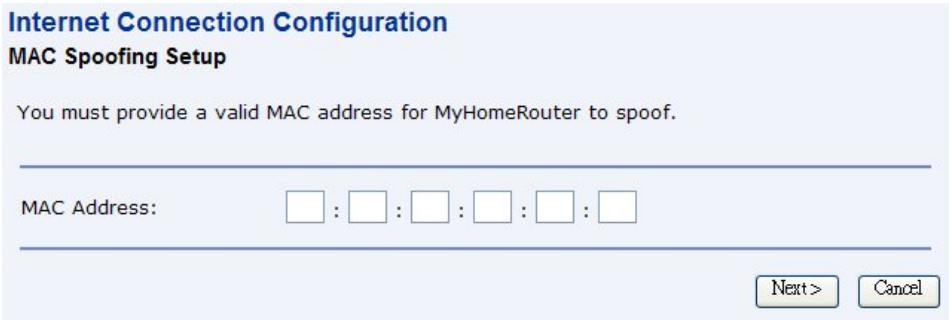


Figure 30: MAC Spoofing Setup

- Click *Next* and *Confirm* to confirm the specified MAC Spoofing settings.

Local Network (LAN) Page

This page allows you to setup the Local Network (LAN) connection. The following are the types of settings allowed:

IP Address
DNS Client
DNS Relay
DNS LAN Host

Click on Local Network under Configuration from the left-hand side pane. The following page opens:

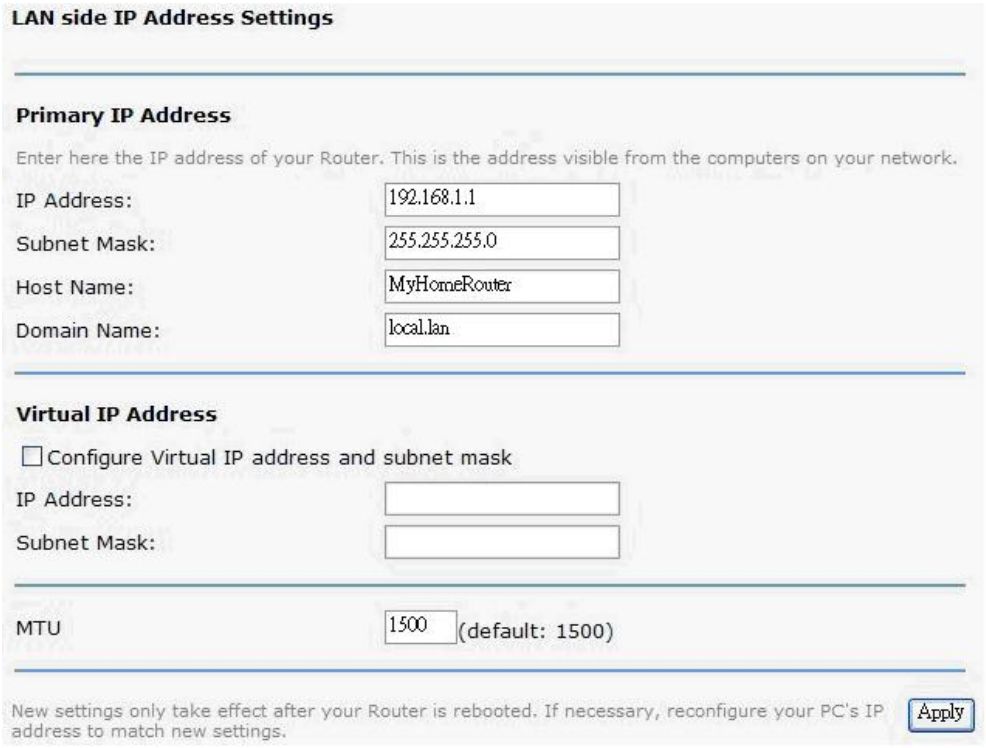

LAN side IP Address Settings
Primary IP Address
Enter here the IP address of your Router. This is the address visible from the computers on your network.
IP Address:
192.168.1.1
Subnet Mask:
255.255.255.0
Host Name:
MyHomeRouter
Domain Name:
local.lan
Virtual IP Address
Configure Virtual IP address and subnet mask
IP Address:
Subnet Mask:
MTU
1500
(default: 1500)
New settings only take effect after your Router is rebooted. If necessary, reconfigure your PC's IP address to match new settings.
Apply

Figure 31: Local Network Configuration - IP address

IP Address

This page displays the local network configuration allowing you to configure:

- IP Address
- Subnet Mask
- Host Name
- Domain Name
- Secondary IP Address and Subnet Mask
- MTU

DNS Client

To specify DNS Client:

- Configure the DNS client by specifying the IP address of DNS server.
- Click *Add*.

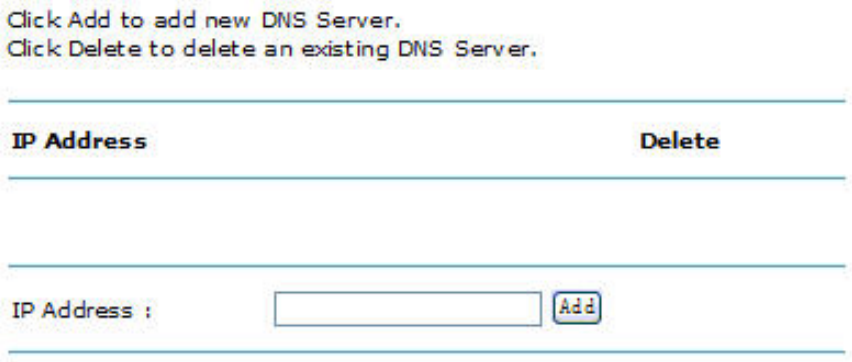


Figure 32: DNS Client

DNS Relay

Click Add to add new DNS Relay Server.
Click Delete to delete an existing DNS Relay Server.
IP Address
Delete
IP Address :
Add

Figure 33: DNS Relay

To add the fixed DNS Relay servers for getting the IP address from domain name:

- Enter the IP address of DNS Relay server.
- Click *Add*

DNS Local Host

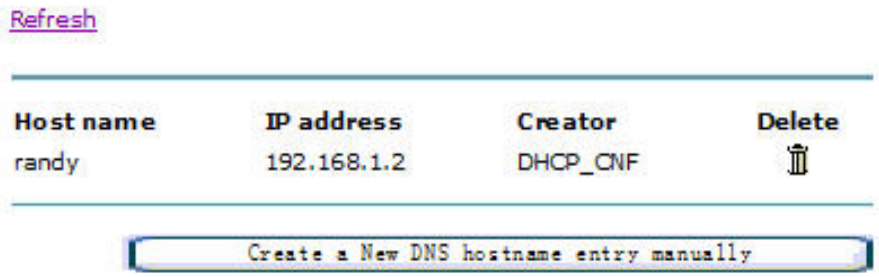


Figure 34: DNS Local Host

Existing local host name and IP address will be shown in this page, you can refresh the details by clicking Refresh.

To create a new DNS Hostname:

- Click *Create a New DNS Hostname entry manually*.
- DNS Table page opens:
- Enter the *Host Name* and *IP Address*.
- Click *Apply*.

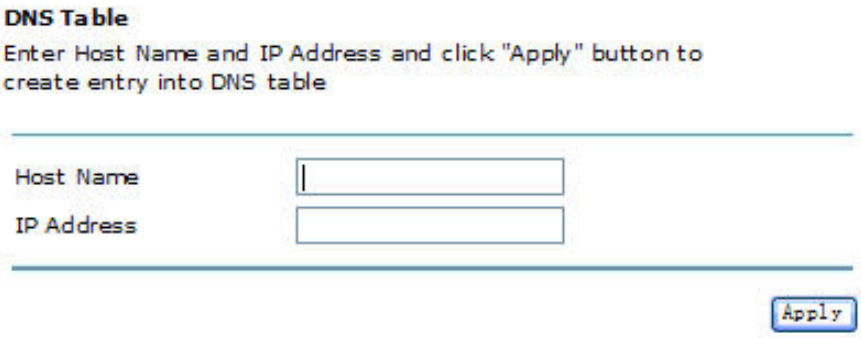


Figure 35: Add New DNS Local Host

DHCP server Page

This page allows you to setup the DHCP server. The following are the types of settings allowed:

Global Settings

Server Settings

Global Settings

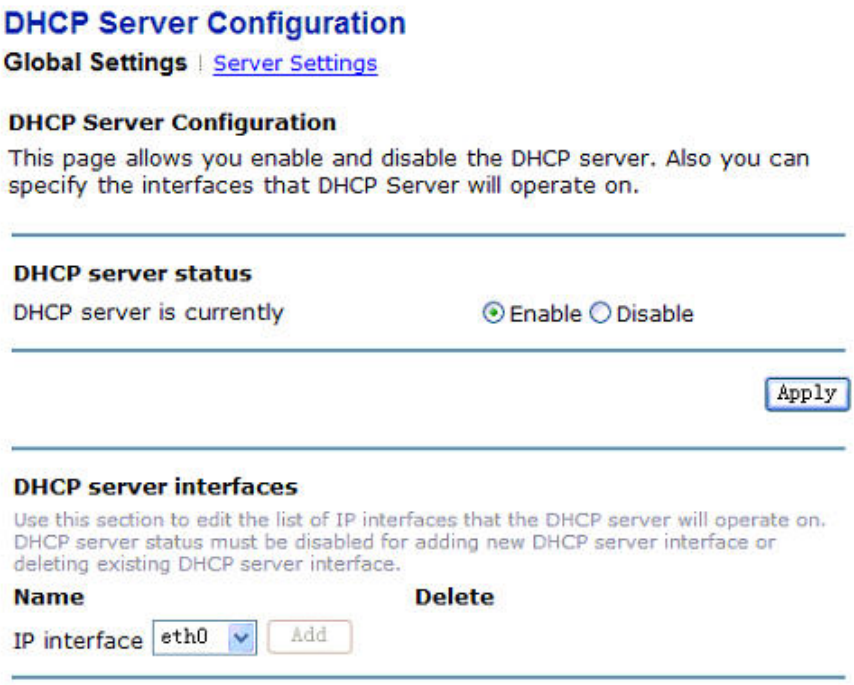

DHCP Server Configuration
Global Settings | Server Settings
DHCP Server Configuration
This page allows you enable and disable the DHCP server. Also you can specify the interfaces that DHCP Server will operate on.
DHCP server status
DHCP server is currently
Enable
Disable
Apply
DHCP server interfaces
Use this section to edit the list of IP interfaces that the DHCP server will operate on. DHCP server status must be disabled for adding new DHCP server interface or deleting existing DHCP server interface.
Name
Delete
IP interface
eth0
Add

Figure 36: DHCP Server Configuration – Global Settings

To configure the DHCP Server:

Global Settings:

- Enable/disable the DHCP server by clicking *Enabled/Disabled*. The current status of the DHCP sever is changed accordingly.
- Specify the *IP Interface* by selecting it from the drop down list and clicking *Add*. Please be noted the DHCP server status must be disabled for adding new DHCP server interface or deleting existing DHCP server interface.

Note

To add an interface, the DHCP Server should be disabled.

Server Settings

This page allows you to create DHCP server subnets and DHCP server fixed host IP/MAC mappings.

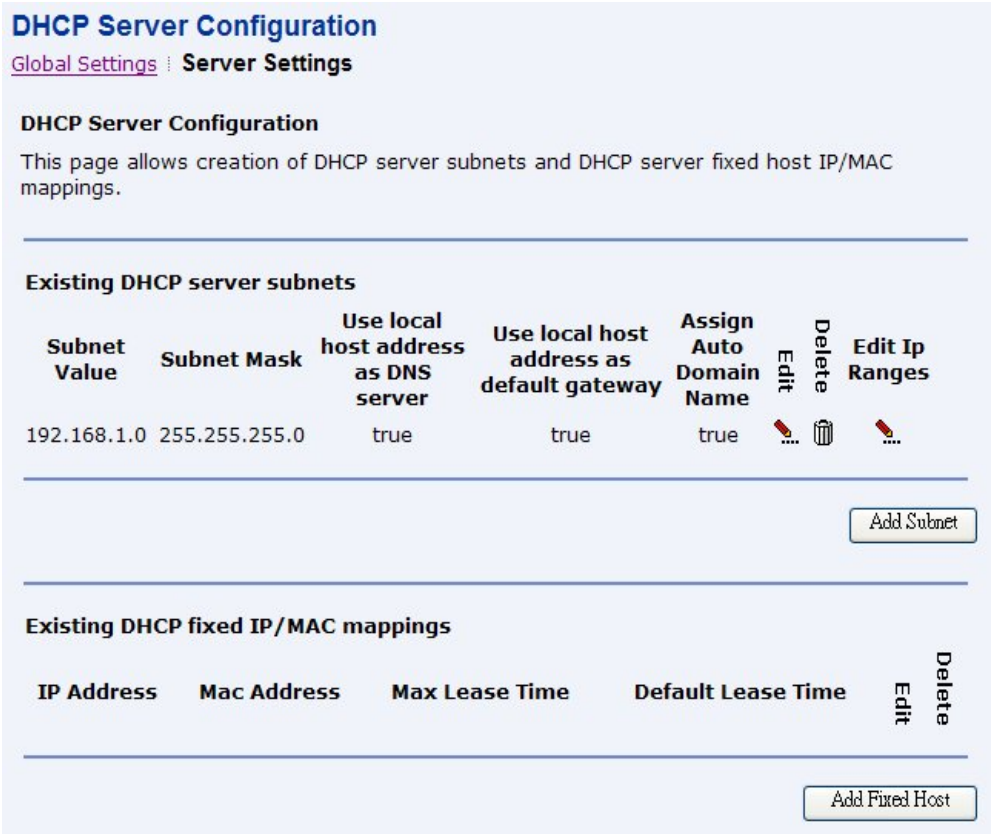


Figure 37: DHCP server Configuration – Server Settings

You may click the *Add Subnet* to open below page.

- Enter the *Subnet value, Subnet mask, Maximum lease time,* and *Default lease time*. By default, the maximum and default lease time are specified as 86400 and 43200 seconds respectively.
- Specify the IP Address range by entering the *Start of address range* and *End of address rang*e. You can select the option *Use a default range*. to specify a default range.
- You may select *Use local host address as DNS server* to allow DHCP server to specify its own IP address.
- You may select *Use local host as default gateway* to specify the local host as default gateway.
- Click *Apply*.

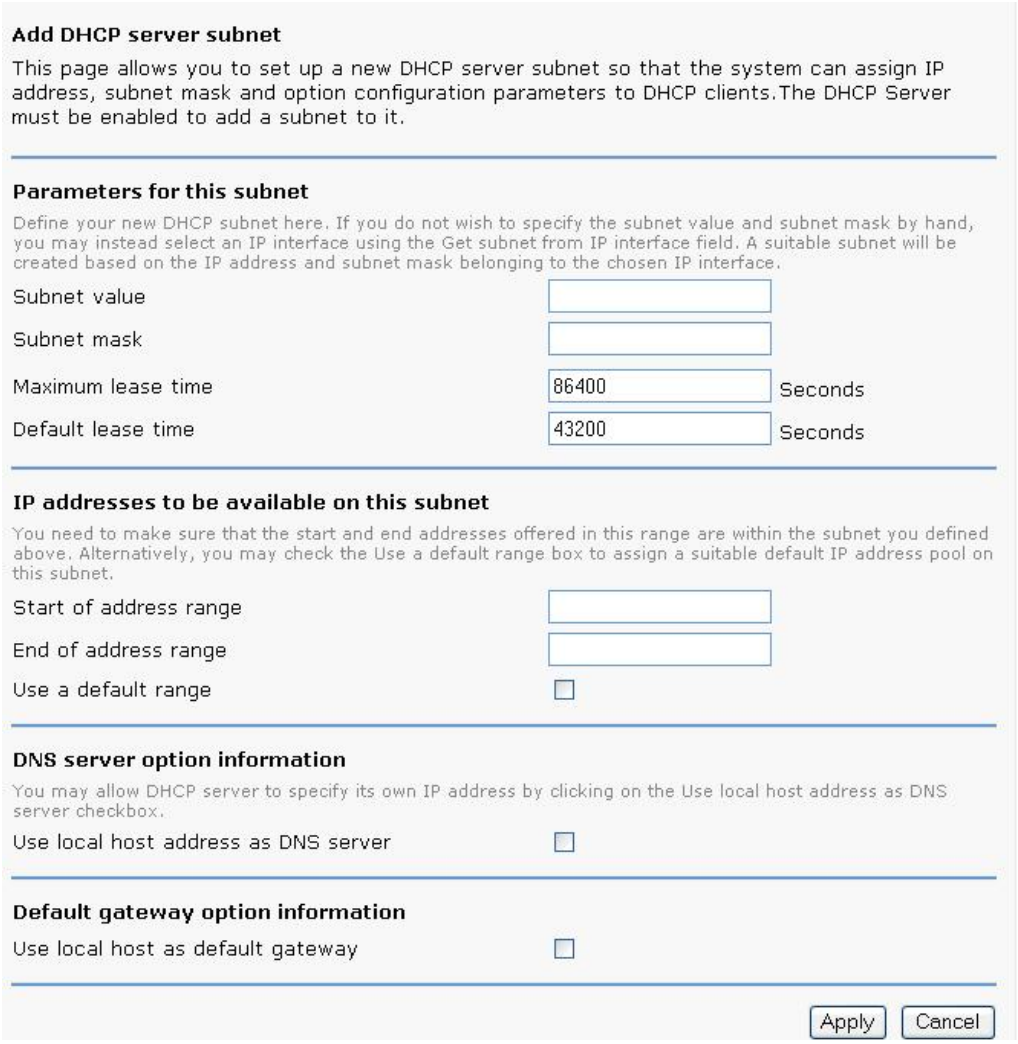

Add DHCP server subnet
This page allows you to set up a new DHCP server subnet so that the system can assign IP address, subnet mask and option configuration parameters to DHCP clients.The DHCP Server must be enabled to add a subnet to it.
Parameters for this subnet
Define your new DHCP subnet here. If you do not wish to specify the subnet value and subnet mask by hand, you may instead select an IP interface using the Get subnet from IP interface field. A suitable subnet will be created based on the IP address and subnet mask belonging to the chosen IP interface.
Subnet value
Subnet mask
Maximum lease time
86400
Seconds
Default lease time
43200
Seconds
IP addresses to be available on this subnet
You need to make sure that the start and end addresses offered in this range are within the subnet you defined above. Alternatively, you may check the Use a default range box to assign a suitable default IP address pool on this subnet.
Start of address range
End of address range
Use a default range
DNS server option information
You may allow DHCP server to specify its own IP address by clicking on the Use local host address as DNS server checkbox.
Use local host address as DNS server
Default gateway option information
Use local host as default gateway
Apply
Cancel

Figure 38: DHCP Server Configuration – Server Subnet Settings

You may click the *Add Fixed Host* to open below page to specify a dedicated IP address for a specified PC (MAC address). Please make sure this IP is in the service range and does not clash an IP address already presented in a dynamic address range.

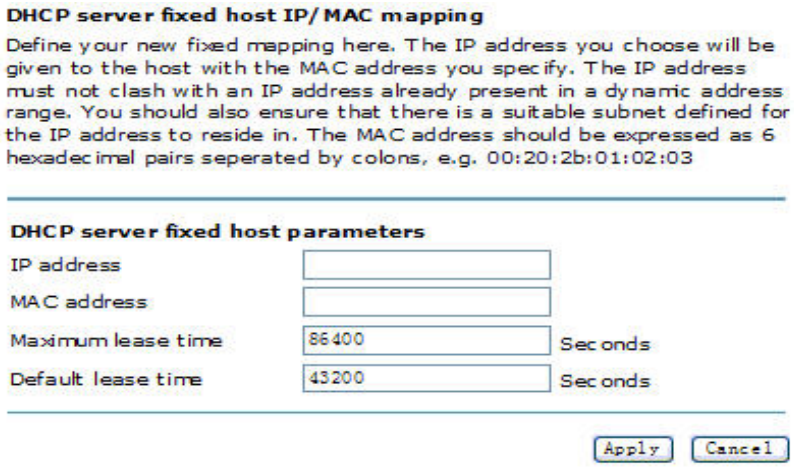

DHCP server fixed host IP/MAC mapping
Define your new fixed mapping here. The IP address you choose will be given to the host with the MAC address you specify. The IP address must not clash with an IP address already present in a dynamic address range. You should also ensure that there is a suitable subnet defined for the IP address to reside in. The MAC address should be expressed as 6 hexadecimal pairs seperated by colons, e.g. 00:20:2b:01:02:03
DHCP server fixed host parameters
IP address
MAC address
Maximum lease time
86400
Seconds
Default lease time
43200
Seconds
Apply
Cancel

Figure 39: DHCP Server Configuration –Fixed Host IP and MAC Mapping

VLAN Configuration

To set the VLAN groups among LAN1, 2, 3, 4 , wireless and wireless1 interfaces, you could group the any port of LAN ports (1 to 4) and then bridge it to other interface group or route it to ADSL WAN port.

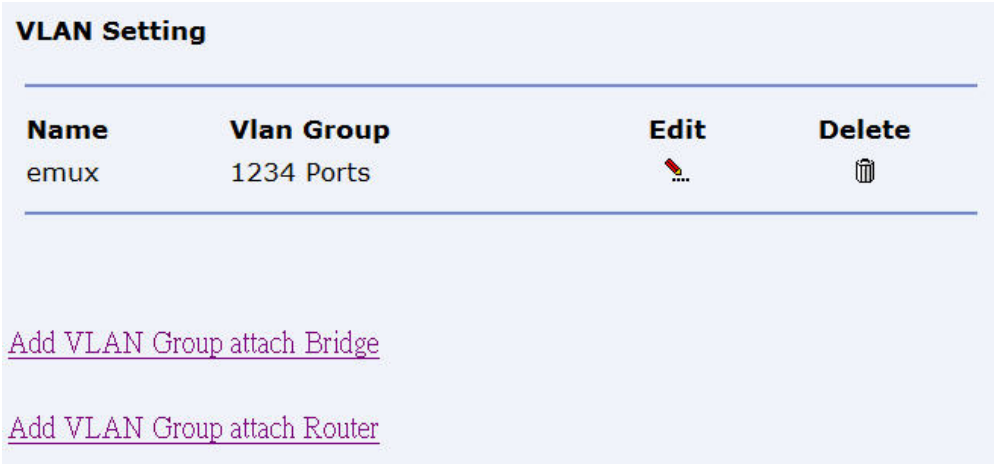


Figure 40: VLAN Configuration – VLAN setting

To click the *Edit* to modify the information of VLAN group and click the *Delete* to delete this entry.

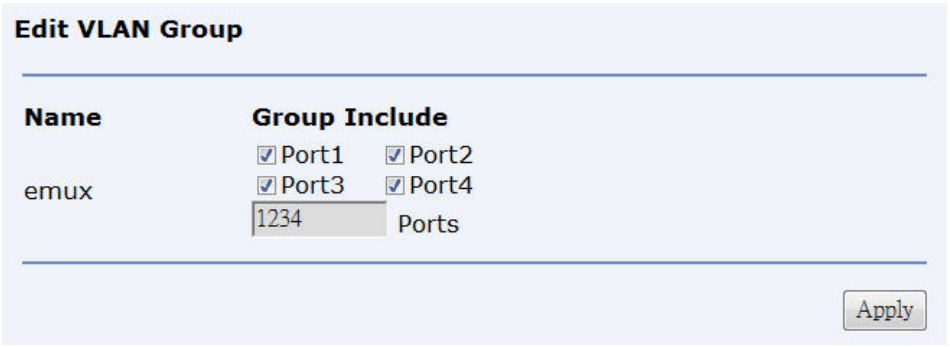


Figure 41: VLAN Configuration – Edit VLAN setting

Click the "*Add VLAN Group Attach Bridge*" to bridge VLAN groups.

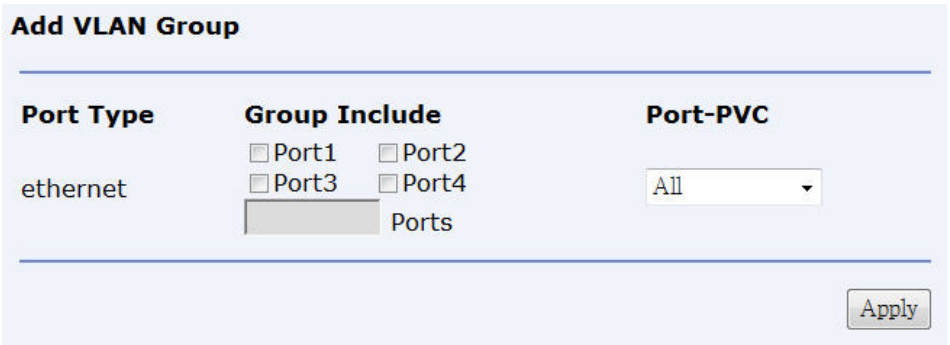


Figure 42: VLAN Configuration – Add VLAN Group - 1

Click the "*Add VLAN Group Attach Route*" to route the VLAN group (LAN port) to ADSL WAN port.

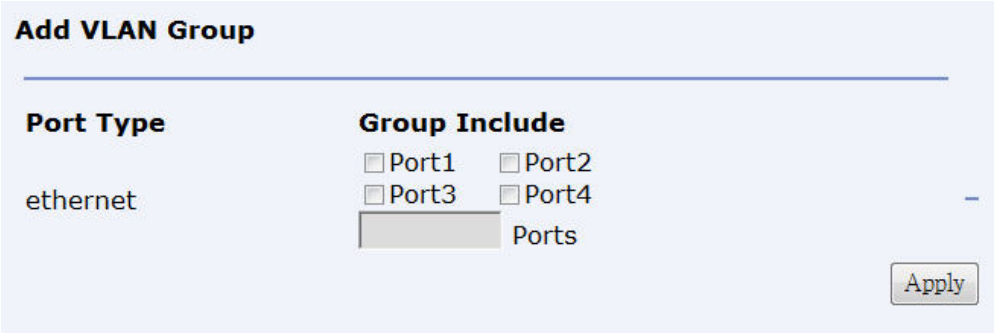


Figure 43: VLAN Configuration – Add VLAN setting - 2

Port - PVC Page

To setup the relationship among those VLAN groups and bridge interfaces, click the selection list to select the VLAN to establish a link between them.

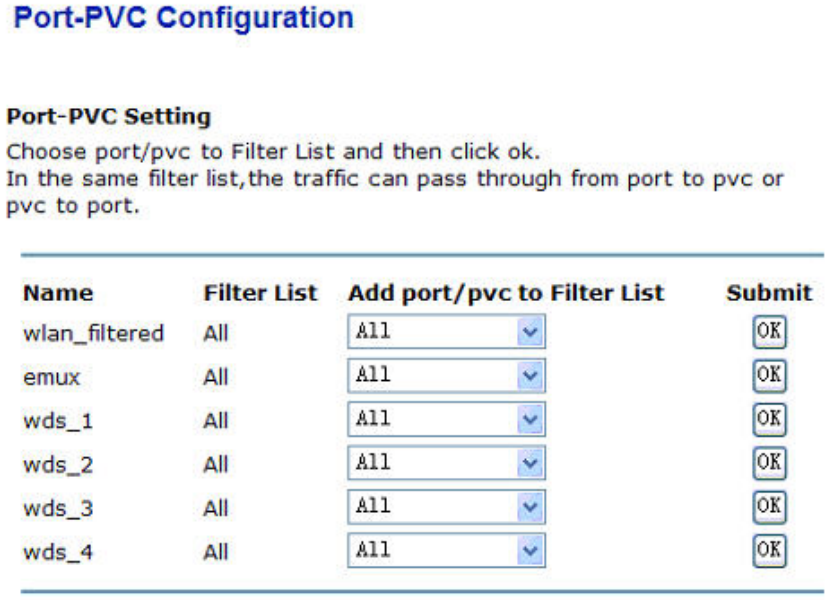

Port-PVC Configuration
Port-PVC Setting
Choose port/pvc to Filter List and then click ok.
In the same filter list,the traffic can pass through from port to pvc or pvc to port.
Name
Filter List
Add port/pvc to Filter List
Submit
wlan_filtered All All OK
emux All All OK
wds_1 All All OK
wds_2 All All OK
wds_3 All All OK
wds_4 All All OK

Figure 44: Port-PVC Configuration

Select the VLAN group and click *OK* to submit your configuration.

7 Security

The Security web page menu includes the following submenus:

IP Filtering
Domain Filtering
Port Forwarding
Virtual Server
MAC Filtering

IP Filtering

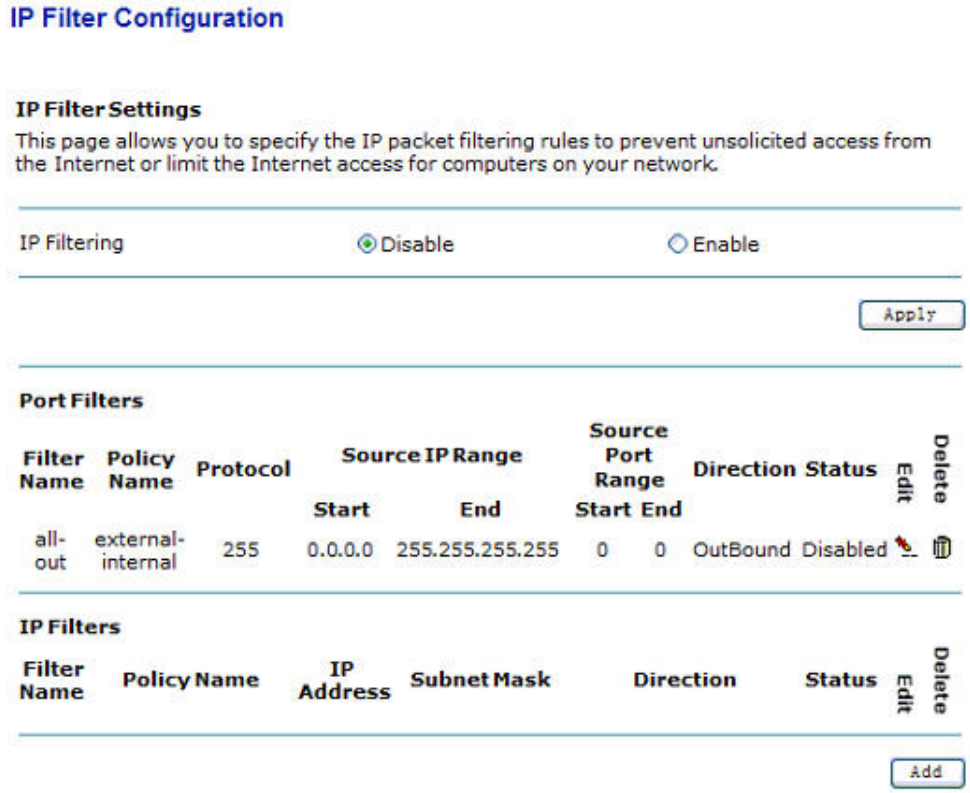


Figure 45: IP Filtering Configuration

IP Filter Settings

To specify the IP filter settings:

- Enable/disable the IP filter by selecting *Enabled/Disabled*.
- Click *Apply*.

Port Filters

Edit or delete the port filters by clicking Edit or Delete. Please refer below page for details.

IP Filters

Add or edit the IP filter by Clicking Add or Edit. Please refer below page for details.

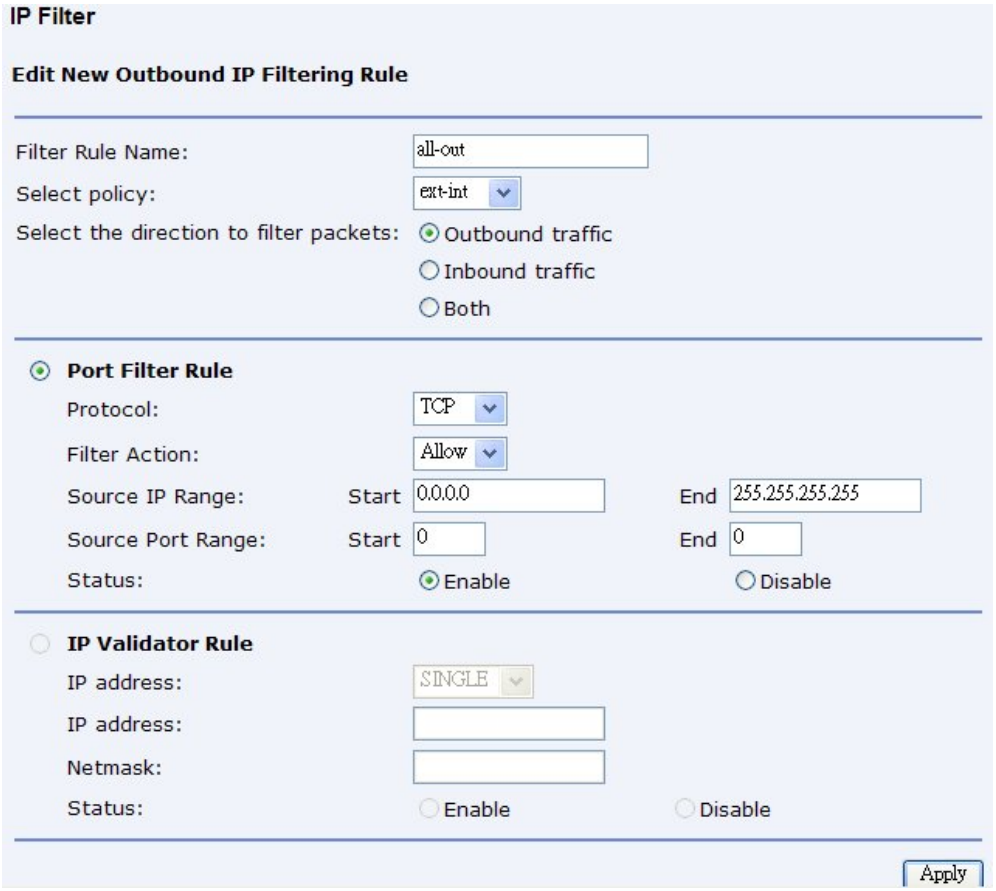


Figure 46: IP Filtering Settings

Global settings:

- Enter the name of filter rule in Filter Rule Name.
- Select the filter policy from the *Select Policy* drop down list.
  - The ext-int means the path is between the WAN port and LAN ports including WLAN port.
  - The ext-dmz means the path is between the WAN port and the specified DMZ port.
  - The dmz-int means the path is between the specified DMZ port and other LAN ports.
- Select one of the option for the direction of filter packets: *Outbound traffic, Inbound traffic, Both.*
- *Specify the Port Filter Rule by specifying the Protocol, Source IP Range, Source Port Range, and Status (Enabled/Disabled).*
- *Specify the IP Validator Rule by specifying the IP Address type (Single, Subnet), IP Address, Netmask, and Status (Enabled/Disabled).*
- *Click Apply.*

Domain Filtering

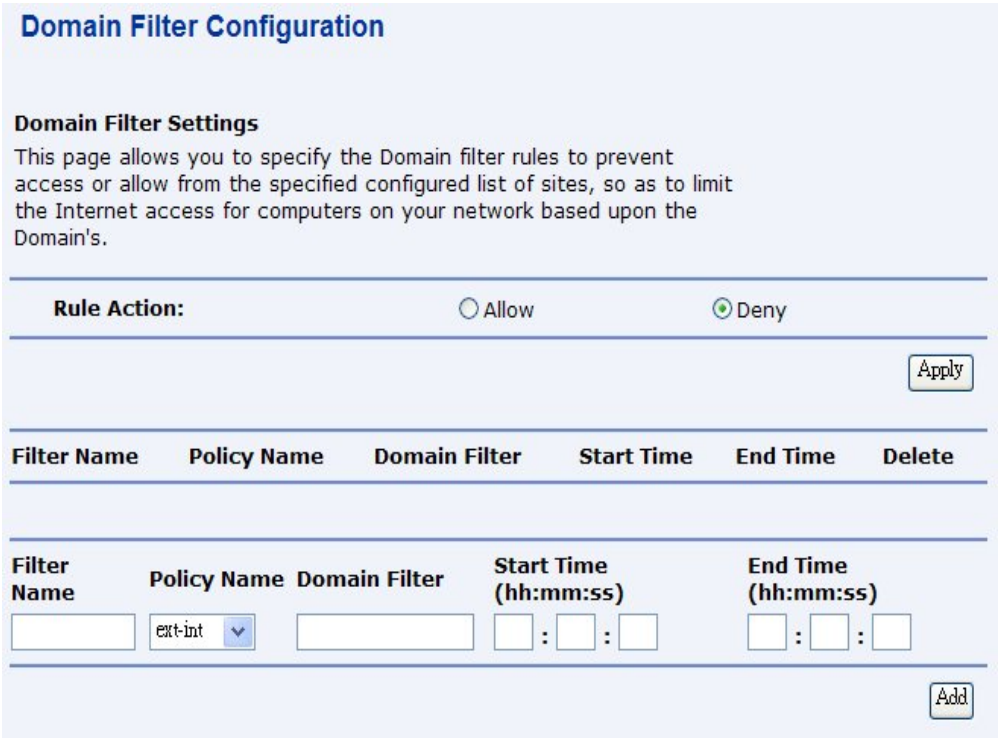


Figure 47: Domain Filtering Configuration

To specify domain filter settings:

- Specify the rule action as *Allow* or *Deny* and click *Apply*.
- Enter the filter details such as *Filter Name*, *Policy Name* (refer the description in IP Filtering), *Domain Filter* (enter the domain name that you want to allow or deny user to surf it), *Start Time (hh:mm:ss)*, *End Time (hh:mm:ss)*.
- Click *Add*.

Port Forwarding Configuration

Port forwarding enables you to run a server on your local network that can be accessed from the Internet. You need to set up port forwarding to tell the device on which computer the server is held. When port forwarding is enabled, your router (the device) routes all the inbound traffic on a particular port to the chosen computer on your network.

Port Forwarding Configuration
Port Forwarding Settings
This page allows to create, modify and delete port forwarding rules. These rules allow applications or software to work on your computers if the Internet connection uses NAT.
Name
Protocol
External Port
Internal IP
Internal Port
Edit
Delete
Add

Figure 48: Port Forwarding Configuration

To configure port forwarding:

- Click *Add*.

Add New Part Forwarding Rule page opens:

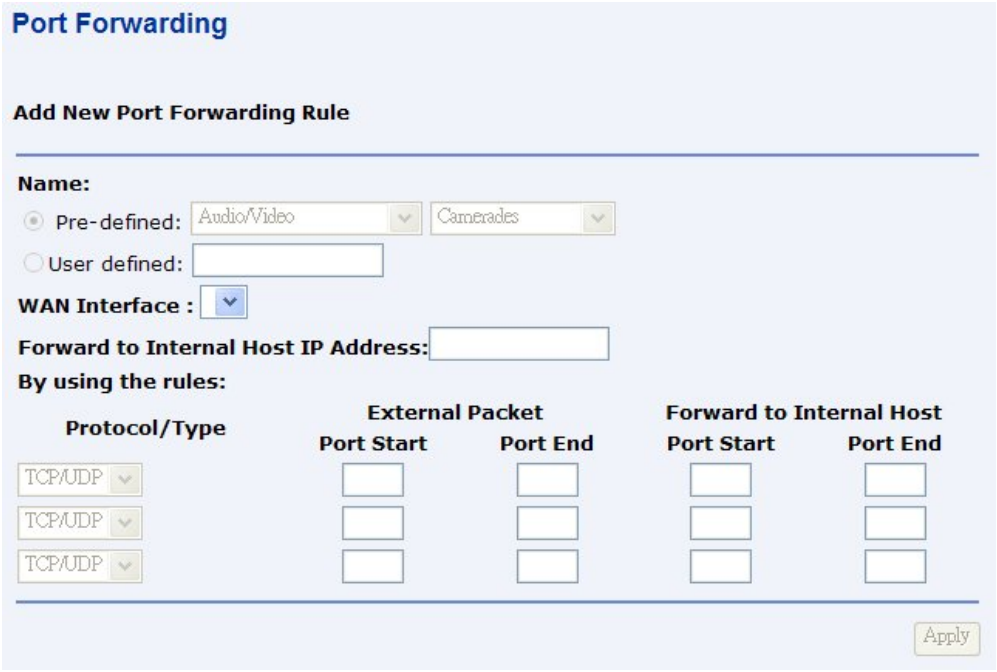


Figure 49: Port Forwarding Settings

- Specify the new port forwarding rule name either by selecting from the *Pre-defined* drop down lists or typing a name in *User defined* text box.
- Select the *WAN Interface* from the drop down list where the incoming packet coming from.
- Enter the IP address in Forward to Internal Host IP Address which the server is held.

- Specify the rules by specifying the information such as Protocol/Type, External Packet (Port Start, Port End), and Forward to Internal Host (Port Start, Port End).
- Click *Apply*.

Virtual Server

A DMZ (DeMilitarized Zone) host is a computer on your network that can be accessed from the Internet regardless of NAT, port forwarding and IP filter settings. A DMZ is often used to host Web servers, FTP servers etc that need to be accessible from the Internet.

Note

Setting up a DMZ has implications on the security of your network. Set-up a DMZ only if you understand the consequences.

Port forwarding settings will override your DMZ setting.

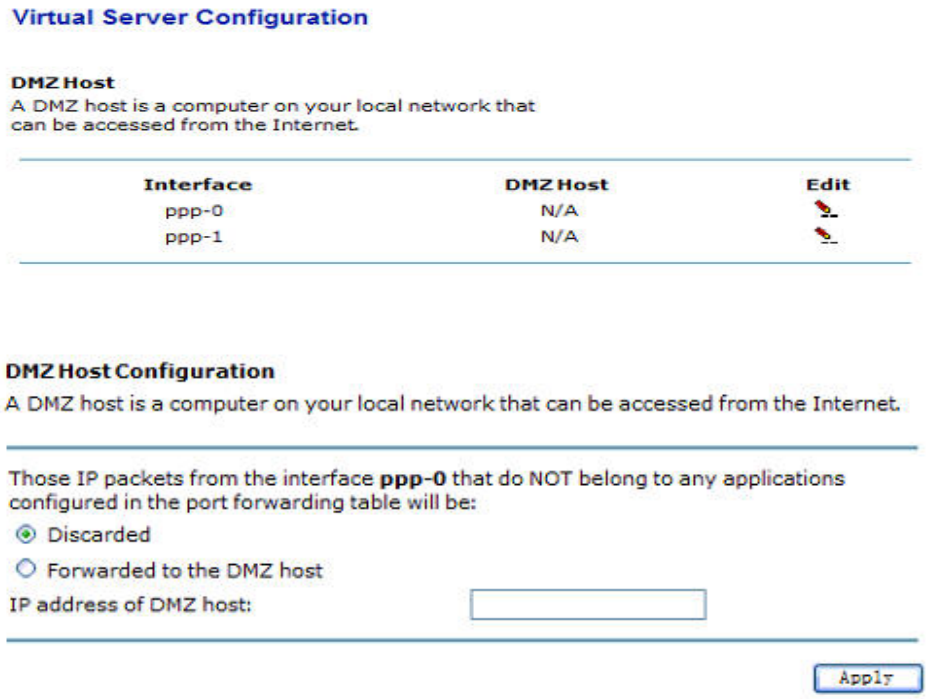

Virtual Server Configuration
DMZ Host
A DMZ host is a computer on your local network that can be accessed from the Internet.
Interface
DMZ Host
Edit
ppp-0
N/A
ppp-1
N/A
DMZ Host Configuration
A DMZ host is a computer on your local network that can be accessed from the Internet.
Those IP packets from the interface ppp-0 that do NOT belong to any applications configured in the port forwarding table will be:
Discarded
Forwarded to the DMZ host
IP address of DMZ host:
Apply

Figure 50: Virtual Server – DMZ Configuration

To setup a DMZ Host:

- Select the WAN interface and click *Edit*.
- Select Forwarded to the DMZ Host
- Enter the IP address of the computer you wish to place in the DMZ
- Click *Apply*.

MAC Filtering

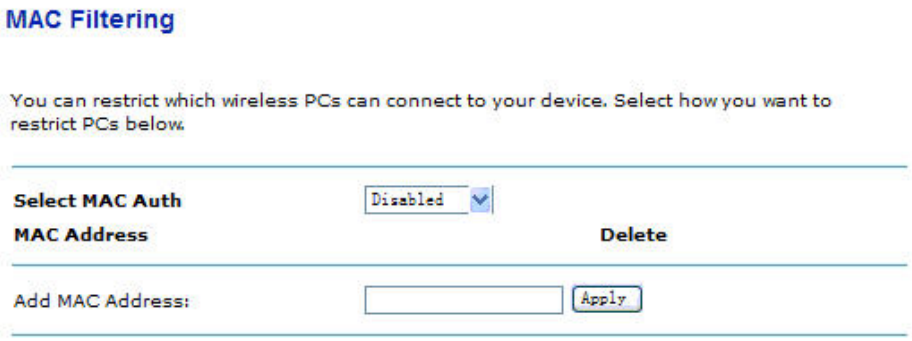

MAC Filtering
You can restrict which wireless PCs can connect to your device. Select how you want to restrict PCs below.
Select MAC Auth
Disabled
MAC Address
Delete
Add MAC Address:
Apply

Figure 51: MAC Filtering Configuration

You can specify which wireless PCs can connect or can not connect to your device.

To setup the MAC filtering feature:

- Select the *MAC Auth* method from Disable (MAC filtering feature is disabled), White List (allow those PCs to connect) or Black List (deny those PCs to connect).
- Enter the MAC address and click *Apply*. You can also delete the existing MAC address by clicking the *Delete*.

8 Services

The Services web page menu includes the following submenus:

IGMP Proxy
IP Routing
Dynamic DNS
Qualify of Service
UPnP

IGMP Proxy

Configure this proxy to run a server on your local network that can be accessed from the Internet. See Help for more information.

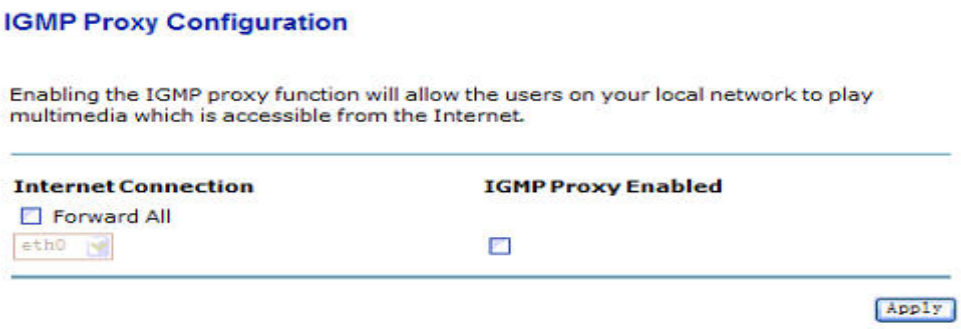

IGMP Proxy Configuration
Enabling the IGMP proxy function will allow the users on your local network to play multimedia which is accessible from the Internet.
Internet Connection
IGMP Proxy Enabled
Forward All
eth0
Apply

Figure 52: IGMP Proxy Configuration

To enable IGMP proxy:

- Select the Forward All to enable IGMP proxy in all interfaces.
- Or select the connection (Interface) from *Internet Connection* drop down list and then enable the IGMP proxy.
- Click *Apply*.

IP Routing

You can configure the packet routing table by static routing or dynamic routing.

Static Routing
Dynamic Routing

Static Routing

Figure 53: IP Routing Configuration

Under static routing web page, click the *ADD* button to add the static routing table.

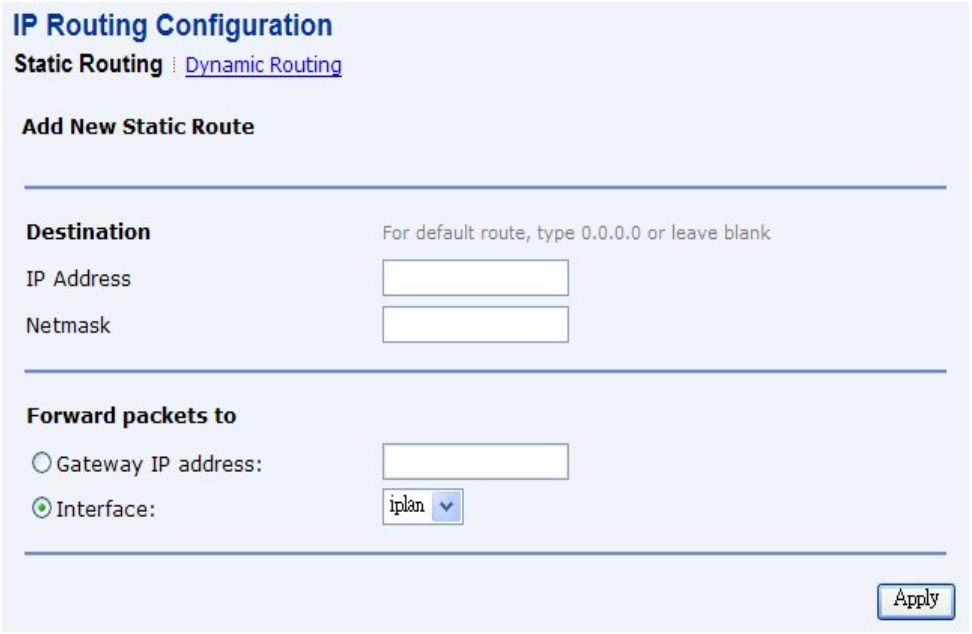


Figure 54: Static IP Routing Configuration

Global settings:

- Specify the destination IP address and its subnet
- Specify the gateway IP address or the interface (LAN or WAN port) where above destination packets to be forwarded

Dynamic Routing

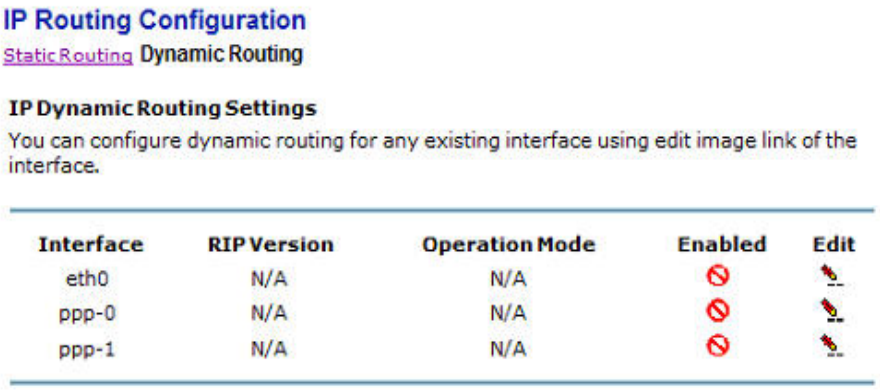


Figure 55: IP Routing - Dynamic IP Routing Configuration

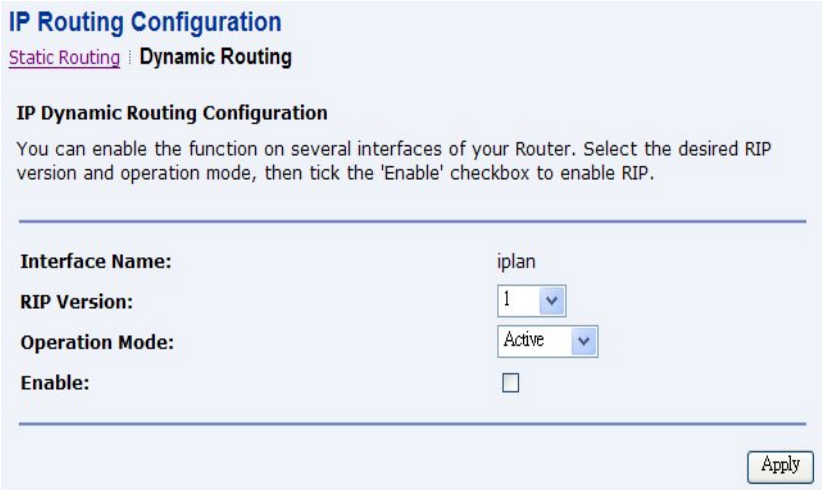


Figure 56: Dynamic IP Routing Configuration

To enable the dynamic routing:

- Select the Interface where to share and exchange the routing table. Click *Edit*.
- Select the *RIP Version* as *1*, *2* or *both*.
- Select the Operation Mode as Active, Passive, or Send Only.
- Select *Enabled*.
- Click *Apply*.

Dynamic DNS

The Dynamic DNS feature allows you to bind the dynamic assigned WAN IP address into a specified domain name. You could pass this domain name to friends to access your service in your site instead of informing them every times if WAN IP address is changed.

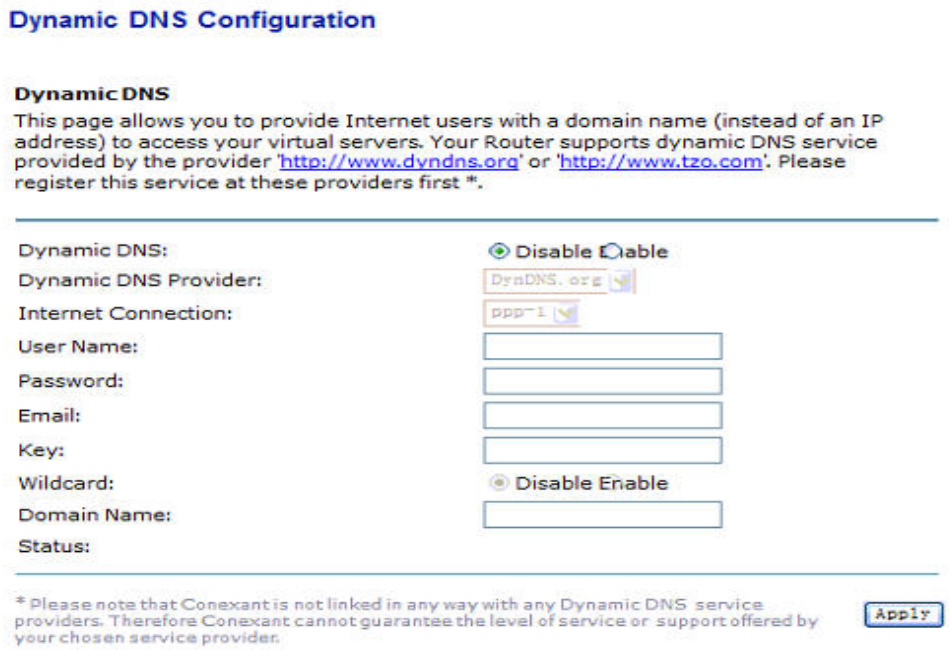

Dynamic DNS Configuration
Dynamic DNS
This page allows you to provide Internet users with a domain name (instead of an IP address) to access your virtual servers. Your Router supports dynamic DNS service provided by the provider 'http://www.dyndns.org' or 'http://www.tzo.com'. Please register this service at these providers first *.
Dynamic DNS:
Disable Enable
Dynamic DNS Provider:
DynDNS.org
Internet Connection:
ppp_1
User Name:
Password:
Email:
Key:
Wildcard:
Disable Enable
Domain Name:
Status:
* Please note that Conexant is not linked in any way with any Dynamic DNS service providers. Therefore Conexant cannot guarantee the level of service or support offered by your chosen service provider.
Apply

Figure 57: Dynamic DNS Configuration

To configure the Dynamic DNS:

- Enable or Disable this Dynamic DNS service.
- Click to select the Dynamic Service Provider.
- Click to select the Internet Connection (WAN port).
- Enter the registered User Name and Password or Email and Key according to the requirement of Dynamic Service Provider.
- Enable or Disable the Wildcard
- Enter the registered Domain Name
- Click the *Apply*

Quality of Service

You can configure the priority of packets through this web page. By default the Classifier details are displayed.

Classifier

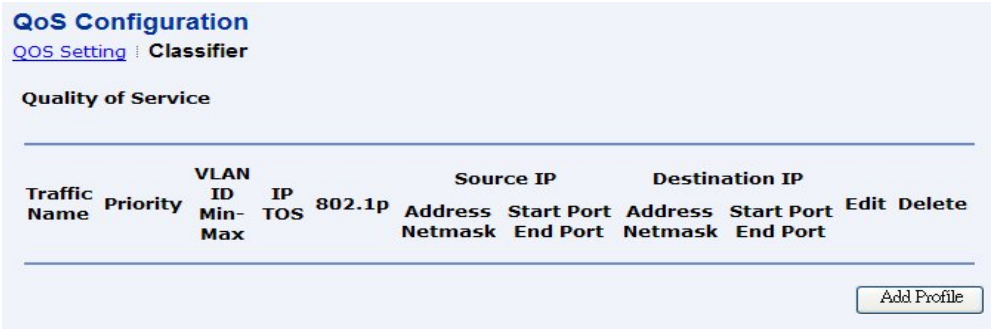


Figure 58: Quality of Service

Click Add Profile to create the packet classifier.

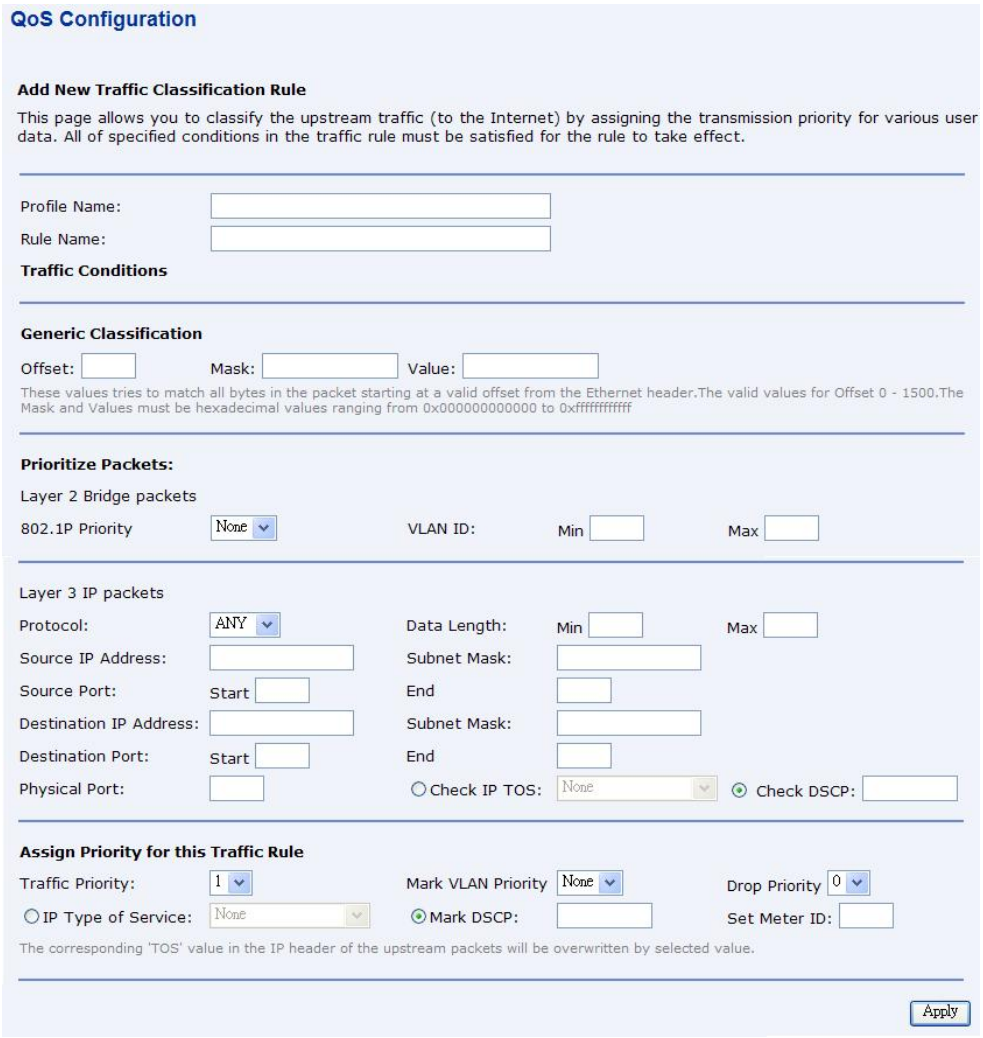


Figure 59: Rule of Quality of Service

Quality of Service, global settings:

- Enter the profile name and rule name for this classifier (rule)
- Generic Classification: These values try to match all bytes in the packet starting at a valid offset from the Ethernet header. The valid values for Offset are 0 - 1500. The Mask and Values must be hexadecimal values ranging from 0x000000000000 to 0xffffffffffff. All the incoming packets will be matched against the configured values of offset, mask and values. If the incoming packet values matches than the configured action will perform.
- Prioritize packets in Layer 2: All the incoming packets will be matched against the configured values of VLAN-ID and VLAN-ID min- max values. If any of the rule matches than the corresponding action will be performed.
  - 802.1p priority bits
  - VLAN ID value
- Prioritize packets in Layer 3: All the incoming packets will be matched against the configured values of the layer 3 fields (source/destination IP address, mask, DSCP values etc.). If any of the rule matches than the corresponding action will be performed.
  - Packet type which is prioritized and data length
  - Source IP address and subnet
  - Source port range from start to end
  - Destination IP address and subnet
  - Destination port range from start to end
  - Enter the physical port
  - Check one of IP TOS (Type of Service) and DSCP
- Assign the traffic priority, Mask VLAN Priority, Drop Priority, Mark IP TOS or DSCP, and set Meter-ID. The corresponding IP TOS in IP header of packet will be overwritten by this new value.
- Click *Apply* to add this QoS rule.

QoS Setting

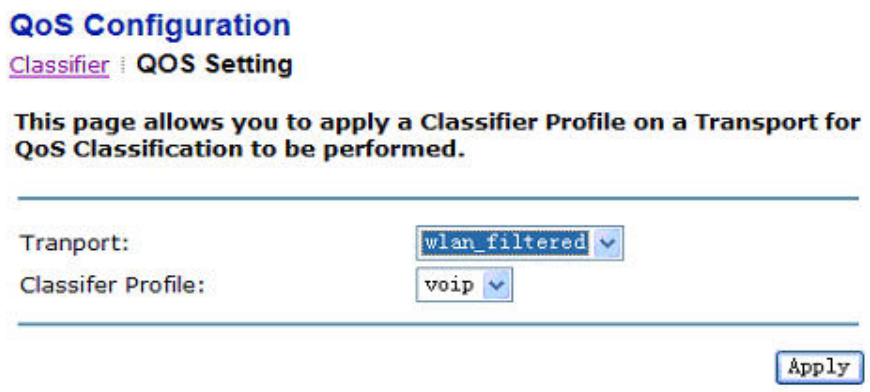


Figure 60: QoS - Attaching Classifier Profile

- Select the transport from *Select the Transport* drop down list.
- Select the classifier profile to be attached to the transport from *Select the Classifier Profile* drop down list.
- Click *Apply*.

UPnP

This page provides you to enable UPnP to help support applications that would not otherwise work behind the device. Both UPnP Internet Gateway Device and NAT Traversal are supported.

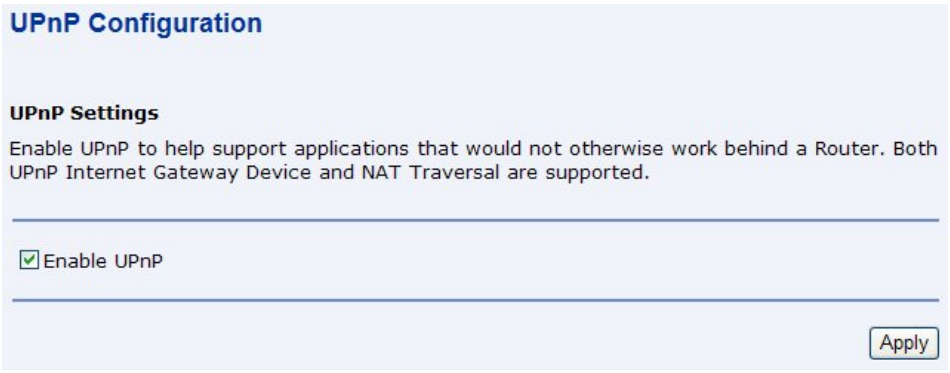

UPnP Configuration
UPnP Settings
Enable UPnP to help support applications that would not otherwise work behind a Router. Both UPnP Internet Gateway Device and NAT Traversal are supported.
Enable UPnP
Apply

Figure 61: UPnP Configuration

To enable or disable the UPnP service:

- Select/unselect *Enable UPnP* to enable/disable the UPnP service
- Click *Apply*.

9 Port Statistics

The Port Statistic web page menu comprises:

DSL (A1)
Wireless
Raw-Ethernet
Ethernet

DSL (A1)

This web page shows the ADSL status in details. If you are interesting in the parameters, please contact technical support to get the description. You can view two types of values for DSL(A1) port statistics. These are:

Basic
Advanced

Basic:

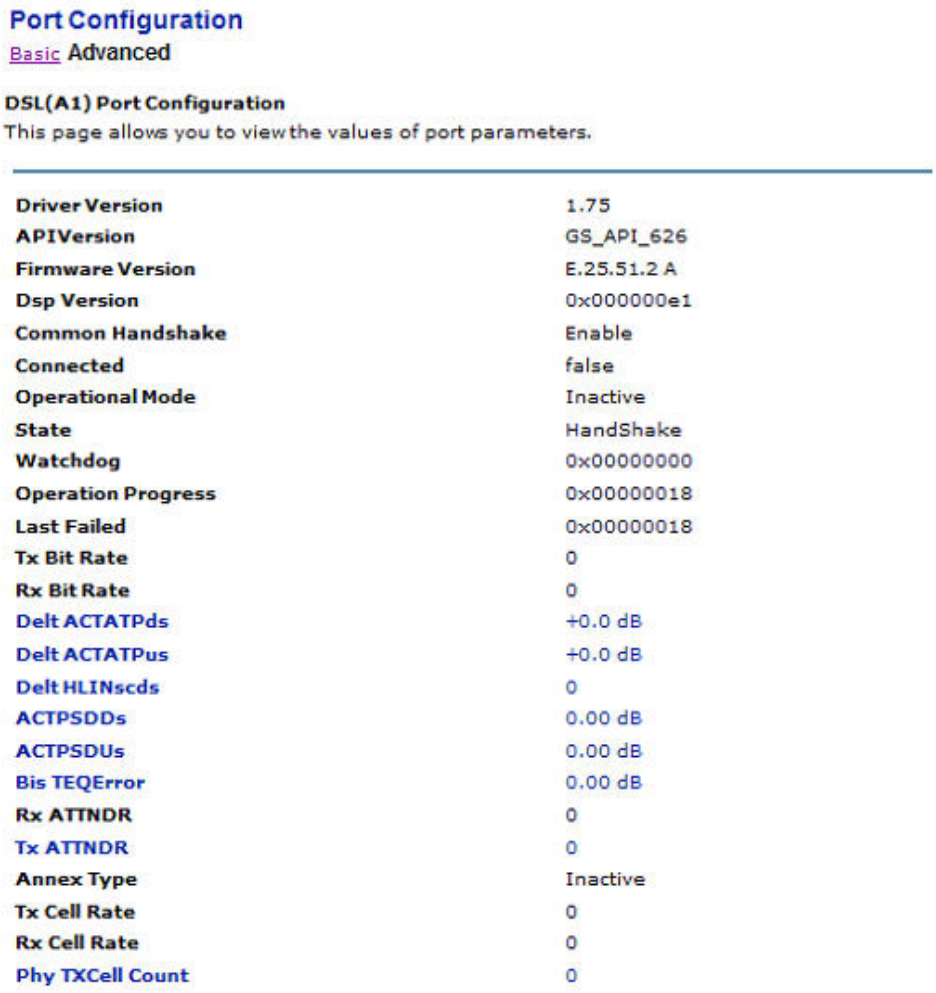
Port Configuration
Basic Advanced

DSL(A1) Port Configuration
This page allows you to view the values of port parameters.

Driver Version	1.75
APIVersion	GS_API_626
Firmware Version	E.25.51.2 A
Dsp Version	0x000000e1
Common Handshake	Enable
Connected	false
Operational Mode	Inactive
State	HandShake
Watchdog	0x00000000
Operation Progress	0x00000018
Last Failed	0x00000018
Tx Bit Rate	0
Rx Bit Rate	0
Rx ATTNDR	0
Annex Type	Inactive
Tx Cell Rate	0
Rx Cell Rate	0
Overall Failure	0
Data Boost	Disable
Local ITUCountry Code	0
INPup	0.0
INPdown	0.0
PMstatus	Unknown (2954)
PSDMask Status	Standard
Status Fail Count	0

Figure 62: View Basic DSL Port Parameters

Advanced:



Port Configuration

Basic Advanced

DSL(A1) Port Configuration

This page allows you to view the values of port parameters.

Driver Version	1.75
APIVersion	GS_API_626
Firmware Version	E.25.51.2 A
Dsp Version	0x000000e1
Common Handshake	Enable
Connected	false
Operational Mode	Inactive
State	HandShake
Watchdog	0x00000000
Operation Progress	0x00000018
Last Failed	0x00000018
Tx Bit Rate	0
Rx Bit Rate	0
Delt ACTATPds	+0.0 dB
Delt ACTATPus	+0.0 dB
Delt HLINscds	0
ACTPSDDs	0.00 dB
ACTPSDUs	0.00 dB
Bis TEQError	0.00 dB
Rx ATTNDR	0
Tx ATTNDR	0
Annex Type	Inactive
Tx Cell Rate	0
Rx Cell Rate	0
Phy TXCell Count	0

Figure 63: View Advanced DSL Port Parameters

Wireless

This web page shows the Wireless status in details. If you are interesting in the parameters, please contact technical support to get the description. You can view two types of values for wireless port statistics. These are:

Basic

Advanced

Basic:

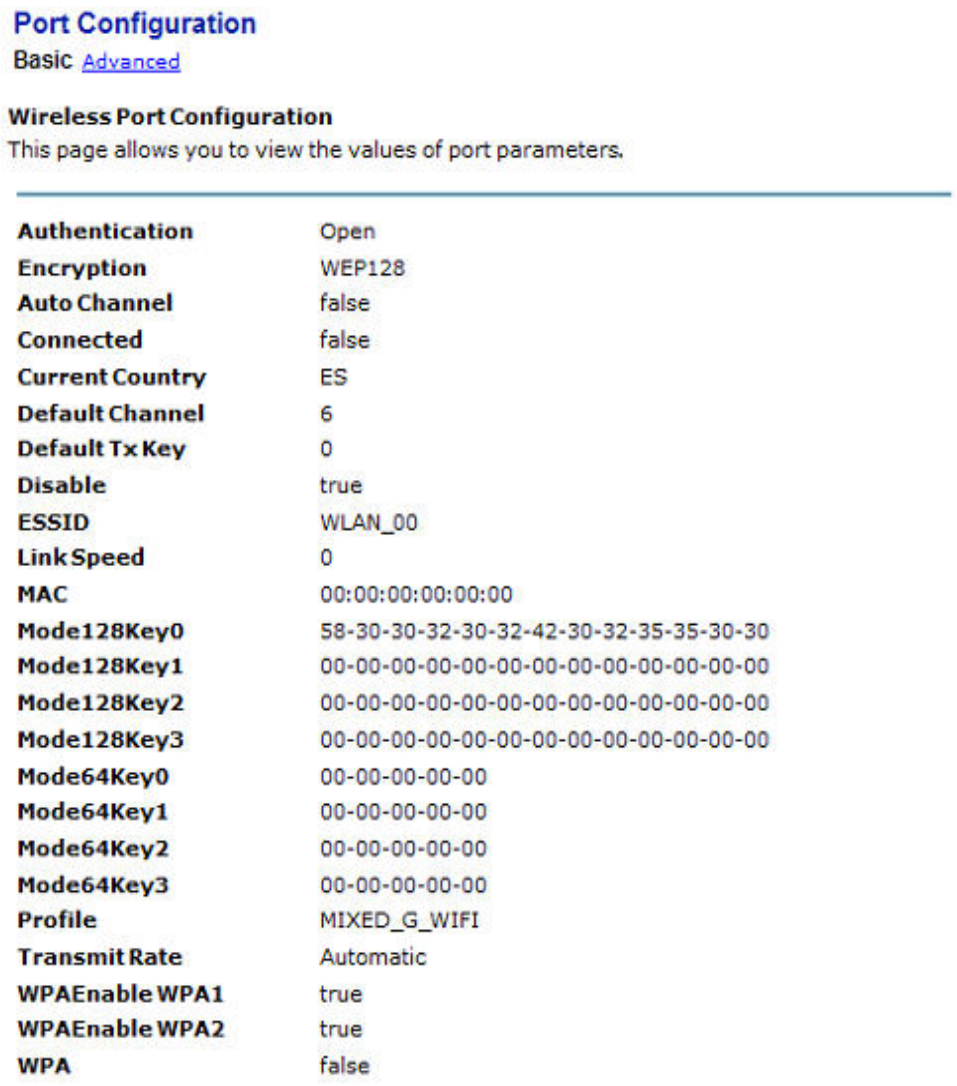


Figure 64: View Basic Wireless Port Parameters

Advanced:

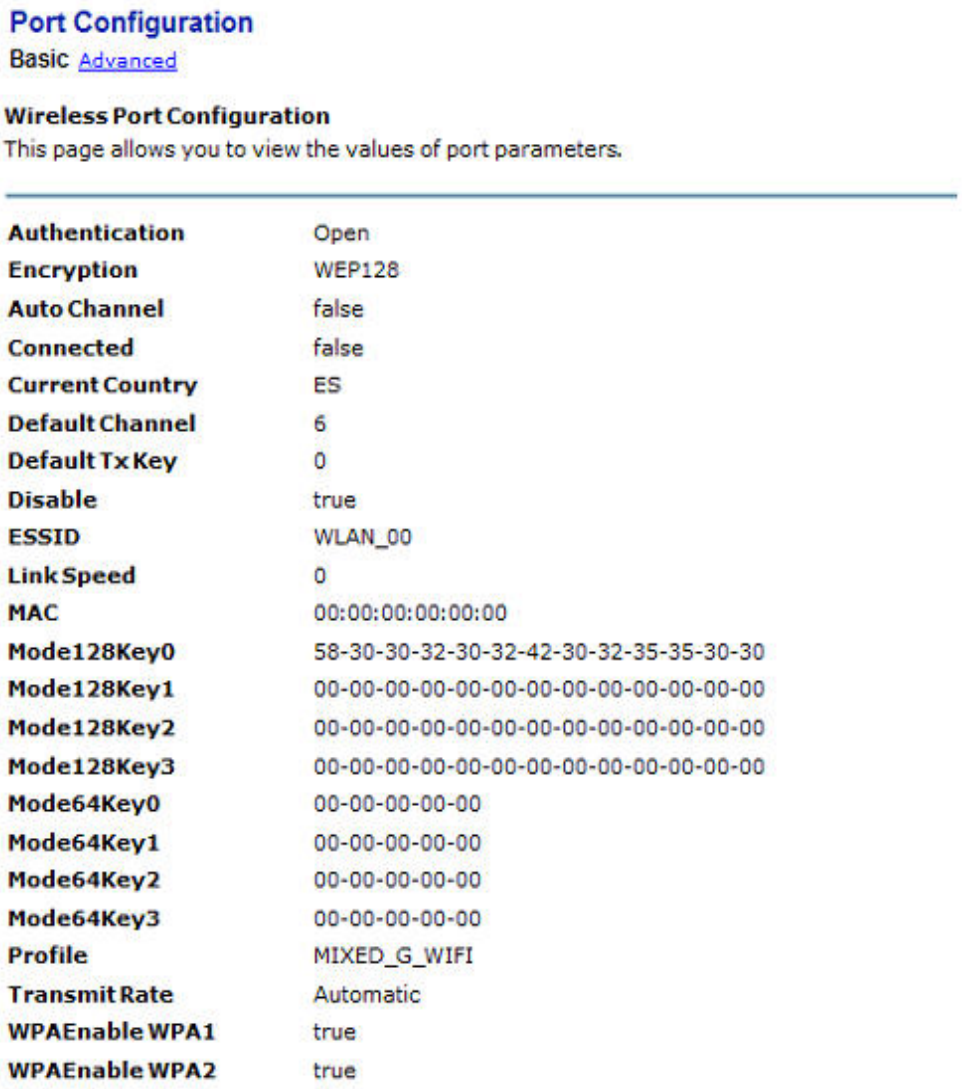


Figure 65: View Advanced Wireless Port Parameters

Raw-Ethernet

This web page shows the raw Ethernet status in details. If you are interesting in the parameters, please contact technical support to get the description. You can view two types of values for raw Ethernet port statistics. These are:

Basic

Advanced

Basic:

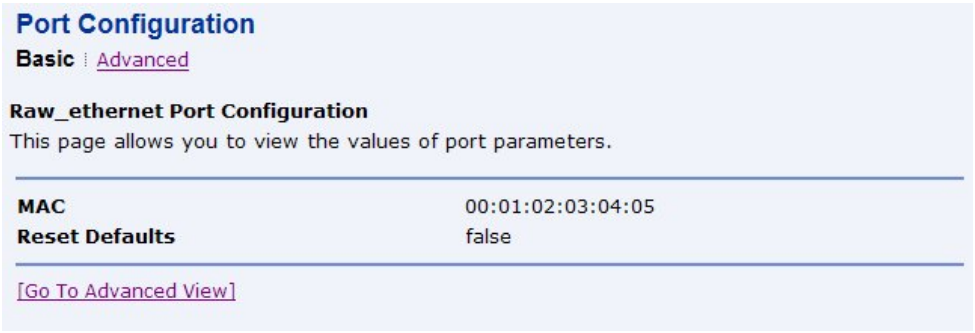

Port Configuration
Basic | Advanced
Raw_ethernet Port Configuration
This page allows you to view the values of port parameters.
MAC 00:01:02:03:04:05
Reset Defaults false
[Go To Advanced View]

Figure 66: View Basic Raw-Ethernet Port Parameters

Advanced:

Port Configuration
Basic | Advanced
Raw_ethernet Port Configuration
This page allows you to view the values of port parameters.
MAC 00:01:02:03:04:05
Max Queue 64
Rx Multicast All Enable true
Max Multicast Listsize 64
Full Duplex Enable true
Promiscuous Enable true
Physical Port 0
Hash High 4294967295
Hash Low 4294967295
Addr 0x30000400
Rx Missed Frames 0
Rx Lockup Fix Applied 0
Rx CRCError 0
Rx Frame Error 0
Rx Overflow Error 0
Rx Short Packet Error 0
Rx Buff Error 0
Rx Not First Error 0
Rx Not Last Error 0
Tx No Carrier Error 0
Tx Excessive Retry Error 0
Tx Underflow Error 0

Figure 67: View Advanced Raw-Ethernet Port Parameters

Ethernet

This web page shows the Ethernet status in details. If you are interesting in the parameters, please contact technical support to get the description. You can view two types of values for Ethernet port statistics. These are:

Basic

Advanced

Basic:

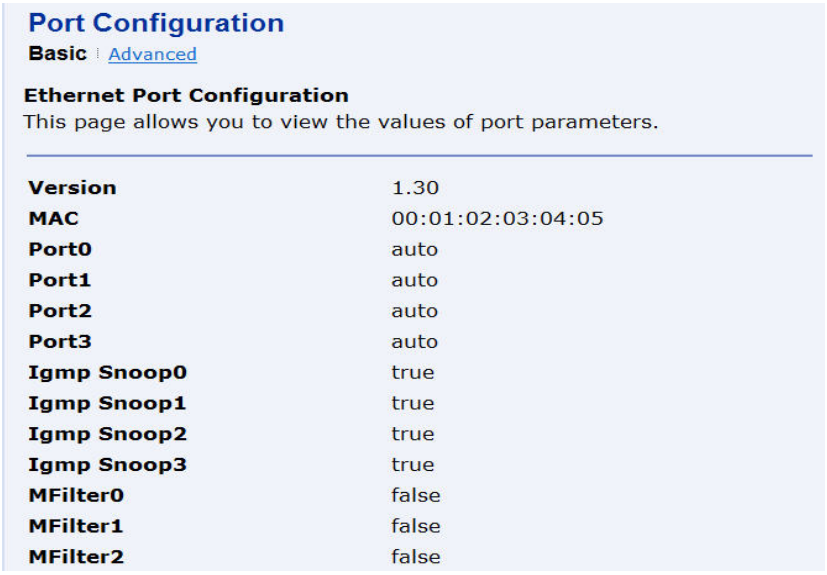


Figure 68: View Basic Ethernet Port Parameters

Advanced:

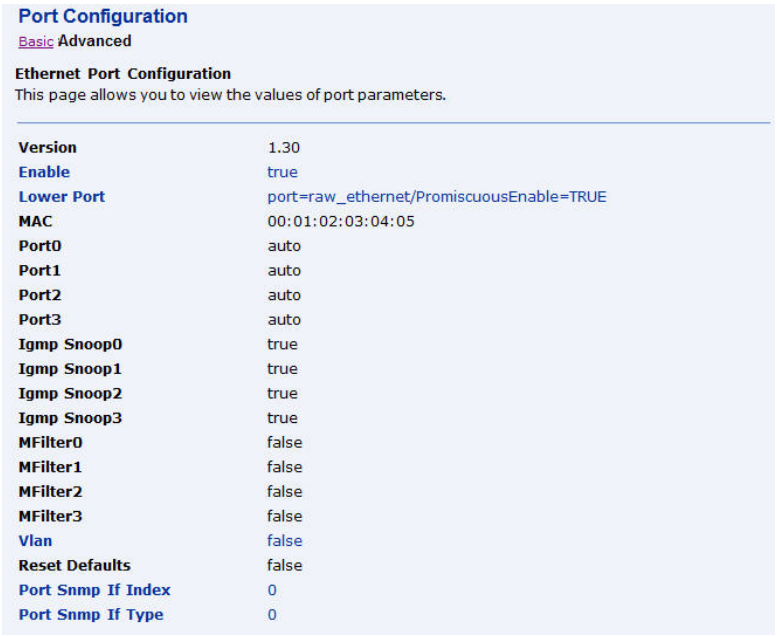


Figure 69: View Advanced Ethernet Port Parameters

10 Admin

The System web page menu comprises:

Firmware Upgrade
Backup & Restore
Reboot
Remote Access
Change Password
Time Zone

Firmware Upgrade

This page displays the current version of the firmware and lets you upgrade to the latest version.

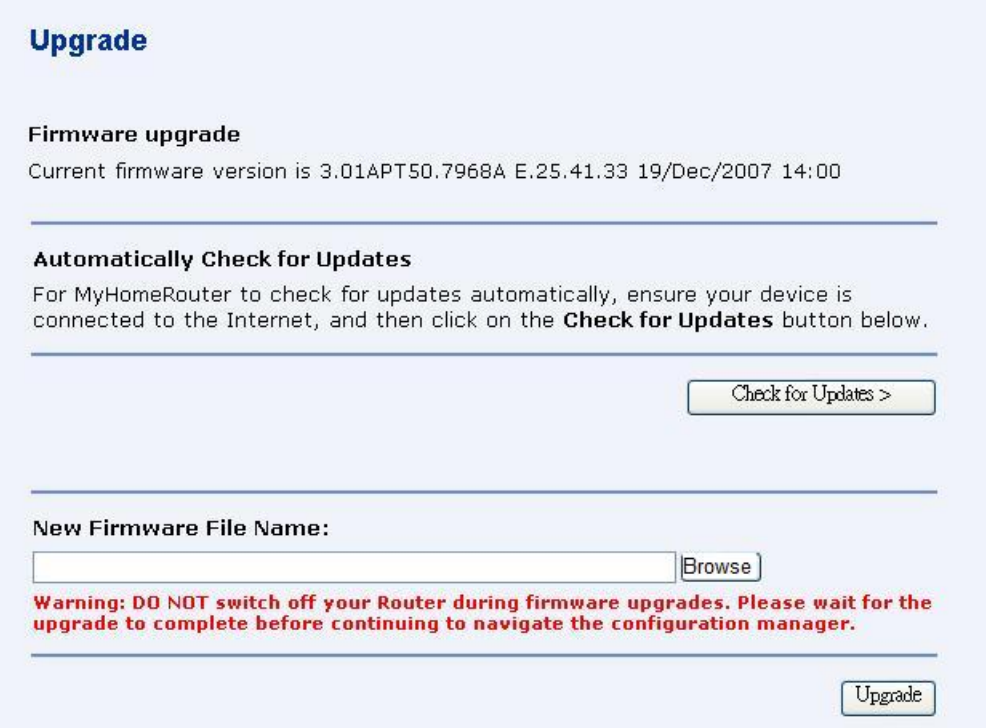

Upgrade
Firmware upgrade
Current firmware version is 3.01APT50.7968A E.25.41.33 19/Dec/2007 14:00
Automatically Check for Updates
For MyHomeRouter to check for updates automatically, ensure your device is connected to the Internet, and then click on the Check for Updates button below.
Check for Updates >
New Firmware File Name:
Browse
Warning: DO NOT switch off your Router during firmware upgrades. Please wait for the upgrade to complete before continuing to navigate the configuration manager.
Upgrade

Figure 70: Upgrading Firmware

To upgrade the firmware, you have two options:

- Automatically check for the updates – Click *Check for Updates* button to pick up the latest updates.
- Specify the location of firmware file – Click *Browse* to specify the path where the firmware files are located and click *Upgrade*.

Backup & Restore

This web page allows you to restart your device or reset all settings to factory default settings.

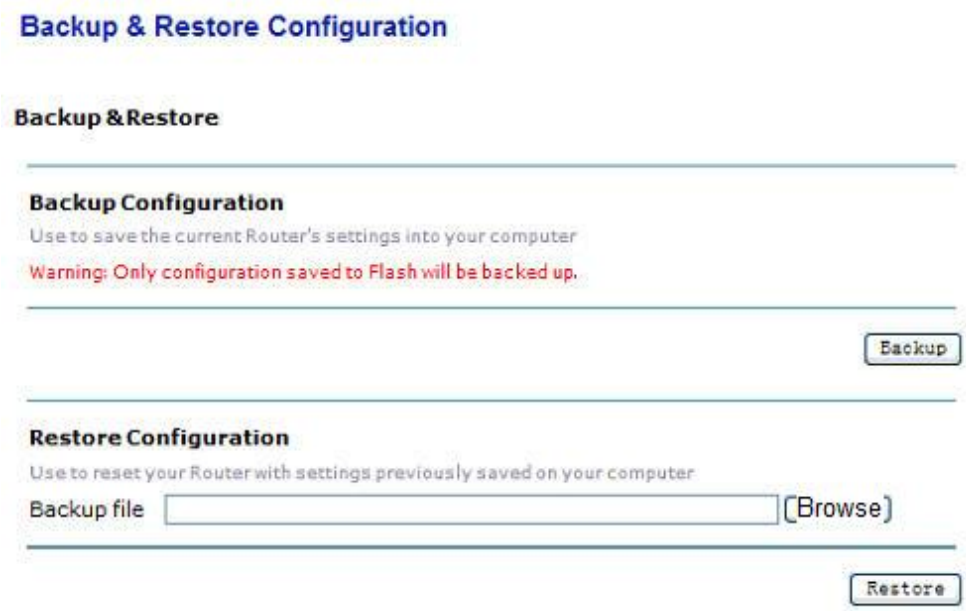
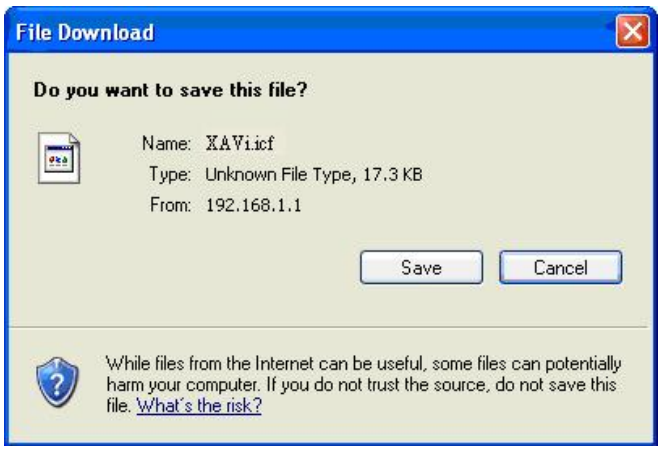

Backup & Restore Configuration
Backup &Restore
Backup Configuration
Use to save the current Router's settings into your computer
Warning: Only configuration saved to Flash will be backed up.
Backup
Restore Configuration
Use to reset your Router with settings previously saved on your computer
Backup file
Browse
Restore

Figure 71: Backup & Restore Configuration

Backup Configuration

To save the backup configuration file:

- Click *Backup*. Please be noted that only configuration saved to flash will be backed up.
- A message window opens prompting you to save the file:


File Download
Do you want to save this file?
Name: XAVi.icf
Type: Unknown File Type, 17.3 KB
From: 192.168.1.1
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

- Click *Save*.

Specify the path where the file is to be saved and click Save.

Restore Configuration

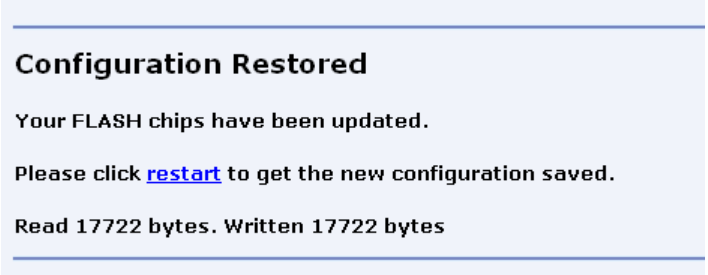
To restore the previously saved configuration:

- Click *Browse* to specify the path of the saved configuration file and click *Open*.
- Click *Upgrade*.

WARNING

Do not restart your router during configuration restore process.

A message appears indicating the status of restoration:


Configuration Restored
Your FLASH chips have been updated.
Please click restart to get the new configuration saved.
Read 17722 bytes. Written 17722 bytes

- Click *restart* to save new configuration.

Reboot

This submenu lets you reboot the modem. You can reboot form the following configurations:

Last Configuration

Factory Configuration

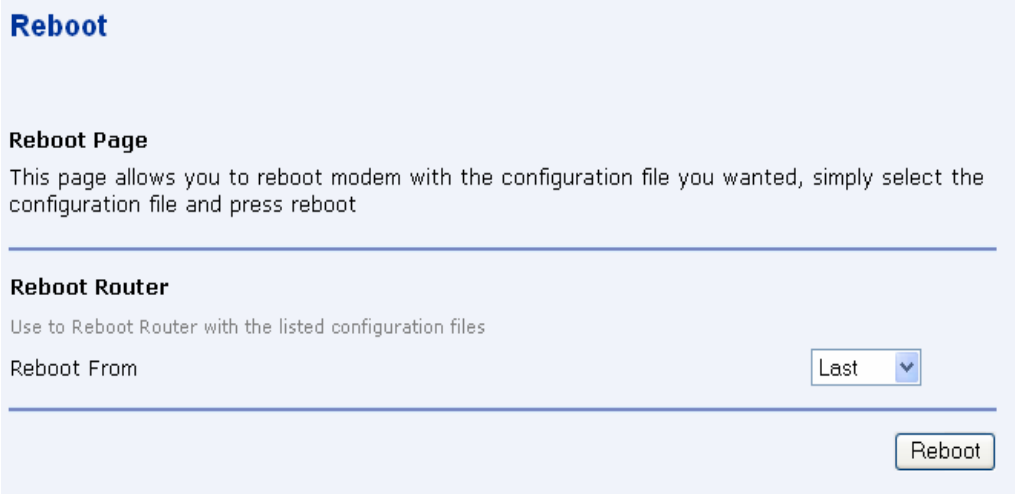

Reboot
Reboot Page
This page allows you to reboot modem with the configuration file you wanted, simply select the configuration file and press reboot
Reboot Router
Use to Reboot Router with the listed configuration files
Reboot From
Last
Reboot

Figure 72: Reboot the Device

To reboot the modem:

- Select *Reboot From* as *Last* or *Factory*.
- Click *Reboot*.

A message appears displaying the status of rebooting:

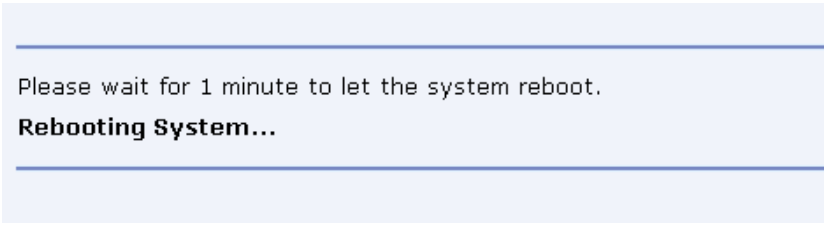


Figure 73: Reboot Status

A page displaying the overview of device information opens.

Remote Access

This submenu provides you remote access to a router. This may help the IT support staff to configure the router remotely.

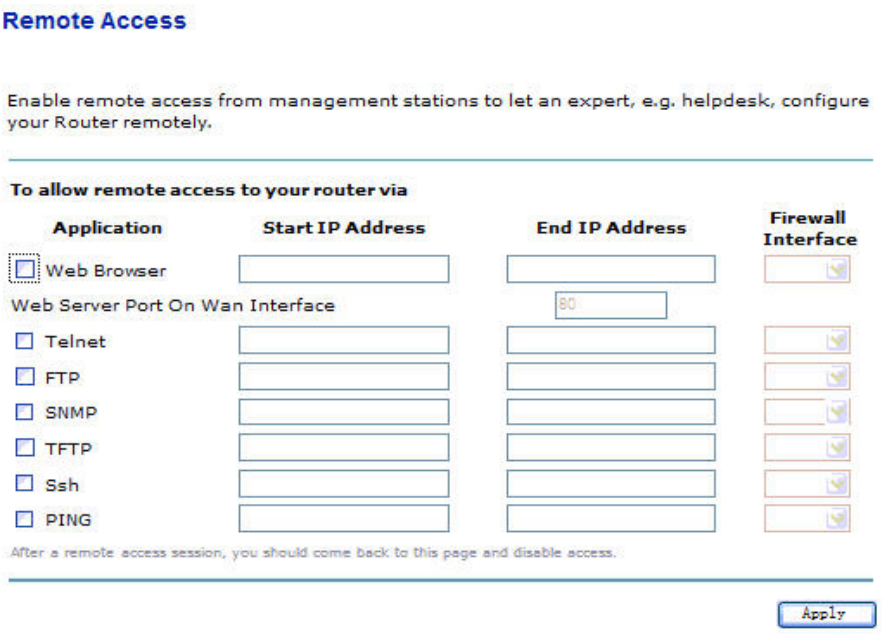


Figure 74: Remote Access Configuration

To enable the remote access:

- Specify the method by which you wish to access the router remotely by selecting it. The following are the methods available for remote access:
  - Web Browser
  - Telnet
  - FTP
  - SNMP
  - TFTP
  - Ssh
  - PING
- Specify the *Start IP Address* and *End IP Address* for the selected method.
- Select the Interface that handles this remote access traffic from *Firewall Interface*.
- Click *Apply*

Change Password

This web page lets you change the user name and password.

Administration Password
It is advisable that the password is changed to keep your system secure. Keep a copy of your password somewhere safe. If you forget your password, your Router will need to be reset and all settings will be lost.
User name:
New password:
Confirm new password:
Make a note of your new password somewhere safe for future reference
Apply

Figure 75: Administration Password Configuration

To change the password:

- Select the user name in *User name*.
- Enter the *New Password*
- Confirm the password by retyping it in *Confirm New password*.
- Click *Apply*.

A window opens prompting you re-login with your new username or password:

- Click *OK*.

Time Zone

This submenu lets you configure the SNTP client and server settings. By default, SNTP Client Configuration page opens when you click this submenu.

SNTP Client

SNTP Server

SNTP Client:

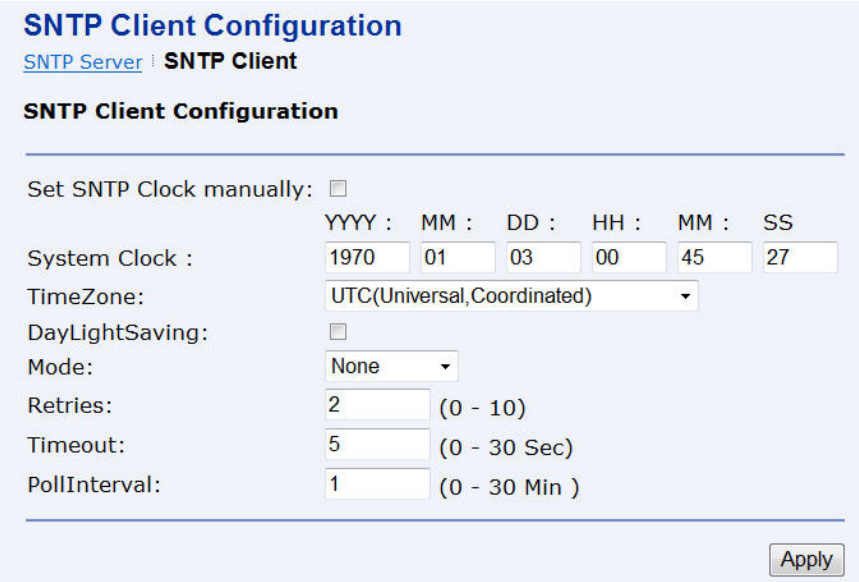


Figure 76: SNTP Client Configuration

To configure the SNTP client:

- Select *Set the Clock Manually* and specify the time in *System Clock* in YYYY:MM:DD:HH:MM:SS format.
- Select the *Time Zone* from the drop down list
- Specify whether the day light savings applies by selecting *Day/Light Savings*.
- Specify the *Mode* by selecting it from the drop down list. The available modes are: *None, Unicast, Broadcast, and Anycast*
- Specify the retry time, timeout, and poll interval in *Retries*, *Timeout*, and *PollInterval* respectively. The time range is specified against each of these fields
- Click *Apply*.

SNTP Server:

Figure 77: SNTP Server Configuration

To configure the SNTP client:

- Select one of the options: Host Name or IP Address.
- Enter the required information and click *Add*
- You could click the Delete icon to remove the SNTP entry from the existing list.

11 Appendix A - Configuring the Internet Settings

This appendix provides instructions for configuring the Internet settings on your computers to work with the device.

Configuring Ethernet PCs

Before you begin

By default, the device automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.

Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the device to do so. See

Assigning static Internet information to your PCs section.

If you have connected your LAN PCs via Ethernet to the device, follow the instructions that correspond to the operating system installed on your PC:

- Windows Vista
- Windows XP PCs
- Windows 2000 PCs
- Windows Me PCs
- Windows 95, 98 PCs
- Windows NT 4.0 workstations

If you want to allow Wireless PCs to access your device, follow the instructions in Configuring Wireless PCs below.

Windows Vista PCs

In the Windows task bar, click the *Start* button, and then click *Control Panel*.

Double-click the Network Connections icon.

In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labeled *Local Area Connection*).The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Ensure that the check box to the left of the item labeled *Internet Protocol TCP/IP* is checked and click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.

Click *OK* twice to confirm your changes, and then close the Control Panel.

Windows XP PCs

In the Windows task bar, click the *Start* button, and then click *Control Panel*.

Double-click the Network Connections icon.

In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labeled *Local Area Connection*). The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

Ensure that the check box to the left of the item labeled *Internet Protocol TCP/IP* is checked and click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.

Click *OK* twice to confirm your changes, and then close the Control Panel.

Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

Double-click the Network and Dial-up Connections icon.

In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*. The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

If Internet Protocol (TCP/IP) does not display as an installed component, click *Install.*

In the *Select Network Component* Type dialog box, select *Protocol*, and then click *Add.*

Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

If prompted, click *OK* to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.

In the *Control Panel*, double-click the Network and Dial-up Connections icon.

In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.

In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP),* and then click *Properties*.

In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled Obtain an IP address automatically. Also click the radio button labeled Obtain DNS server address automatically.

Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

In the Windows task bar, click the Start button, point to Settings, and then click Control Panel.

Double-click the Network and Dial-up Connections icon.

In the Network and Dial-up Connections window, right-click the Network icon, and then select Properties. The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled.

If Internet Protocol (TCP/IP) does not display as an installed component, click Add.

In the Select Network Component Type dialog box, select Protocol, and then click Add.

Select Microsoft in the Manufacturers box.

Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click OK. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.

If prompted, click OK to restart your computer with the new settings. Next, configure the PCs to accept IP information assigned by the device.

In the Control Panel, double-click the Network and Dial-up Connections icon.

In Network and Dial-up Connections window, right-click the Network icon, and then select Properties.

In the Network Properties dialog box, select TCP/IP, and then click Properties.

In the TCP/IP Settings dialog box, click the radio button labeled Server assigned IP address. Also click the radio button labeled Server assigned name server address.

Click OK twice to confirm and save your changes, and then close the Control Panel.

Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

Double-click the Network icon. The *Network* dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.

If TCP/IP does not display as an installed component, click *Add.* The Select Network Component Type dialog box displays.

Select *Protocol*, and then click *Add…*The Select Network Protocol dialog box displays.

Click on *Microsoft* in the Manufacturers list box, and then click *TCP/IP* in the Network Protocols list box.

Click *OK* to return to the Network dialog box, and then click *OK* again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

Click *OK* to restart the PC and complete the TCP/IP installation. Next, configure the PCs to accept IP information assigned by the device.

Open the Control Panel window, and then click the Network icon.

Select the network component labeled TCP/IP, and then click *Properties*. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

In the TCP/IP Properties dialog box, click the IP Address tab.

Click the radio button labeled Obtain an IP address automatically.

Click the DNS Configuration tab, and then click the radio button labeled *Obtain an IP address automatically*.

Click *OK* twice to confirm and save your changes. You will be prompted to restart Windows.

Click *Yes*.

Windows NT 4.0 workstations

First, check for the IP protocol and, if necessary, install it:

In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.

In the Control Panel window, double click the Network icon.

In the *Network dialog* box, click the *Protocols* tab. The *Protocols* tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled.

If TCP/IP does not display as an installed component, click *Add.*

In the *Select Network Protocol* dialog box, select *TCP/IP*, and then click *OK*. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

Click *Yes* to continue, and then click *OK* if prompted to restart your computer. Next, configure the PCs to accept IP information assigned by the device.

Open the Control Panel window, and then double-click the Network icon.

In the *Network* dialog box, click the *Protocols* tab.

In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.

In the Microsoft TCP/IP Properties dialog box, click the radio button labeled Obtain an IP address from a DHCP server.

Click *OK* twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

If you are a typical user, you will not need to assign static Internet information to your LAN PCs because your ISP automatically assigns this information for you.

In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called "statically"), rather than allowing the device to assign it. This option may be desirable (but not required) if:

You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).

You maintain different subnets on your LAN (subnets are described in Appendix B).

Before you begin, you must have the following information available:

The IP address and subnet mask of each PC

The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the device. By default, the LAN port is assigned the IP address 192.168.1.1. (You can change this number or another number can be assigned by your ISP.)

The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place them in the same subnet as the device*'s LAN port.*

Configuring Wireless PCs

You need to configure the operating system installed on your Wireless PCs using the same procedure described for Configuring Ethernet PCs section.

Positioning the wireless PCs

The wireless network cards used determine the maximum distance between your wireless PCs and your device. Guidelines on positioning the hardware components of your wireless network should be provided by your network card provider.

Wireless PC cards and drivers

Each PC on your wireless LAN must be fitted with a wireless access card. You must also install the corresponding driver files for your particular wireless card on your PC. You should receive driver files and instructions on how to install them together with your wireless card.

Configuring PC access to your Wireless device

Before you start configuring your Wireless PC, you must ensure that you have:

A Wireless access card for each of the PCs

Corresponding wireless access card driver software files

The configuration steps below will vary depending on both the operating system and wireless card installed on the PC. These steps provide a basic outline, however you should refer to the documentation provided with your wireless access card for specific instructions.

To configure Wireless PCs:

Install the wireless access card.

Install the wireless driver software files.

Configure the following wireless parameters on each of the wireless PCs:

- Set the adapter to use infrastructure mode. This configures the PCs to access each other and the Internet via the device.
- Configure the SSID and channel to match the SSID and channel previously configured on the device.

Your wireless network can now communicate with the Internet via the device.

12 Appendix C - IP Addresses, Network Masks, and Subnets

IP Addresses

Note

This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called dotted decimal notation. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information:

Network ID
Identifies a particular network within the Internet or intranet

Host ID
Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's class (see following section). The table below shows the structure of an IP address.

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)
Class B: 129.88.16.49 (network = 129.88, host = 16.49)
Class C: 192.60.201.11 (network = 192.60.201, host = 11)

Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

The class can be determined easily from field1:
field1 = 1-126: Class A
field1 = 128-191: Class B
field1 = 192-223: Class C
(field1 values not shown are reserved for special uses)

A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet masks

Definition
mask

A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."

Subnet masks are used to define subnets (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field3 are part of the network ID, but note how the mask specifies that the first bit in field4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 1 to 62.

Note

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

Class A: 255.0.0.0
Class B: 255.255.0.0
Class C:255.255.255.0

These are called default because they are used when a network is initially configured, at which time it has no subnets.

13 Appendix D - Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the device, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the device and a wall socket/power strip.
PPP LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable (called an RJ-11 cable) like the one provided is securely connected to the DSL port and your wall phone port. Allow about 30 seconds for the device to negotiate a connection with your ISP.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the device. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
Internet Access	
My PC cannot access the Internet	Run a health check on your device. Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: ● Check that the gateway IP address on the computer is your public IP address (see Current Status on page 1 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. ● Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.
My LAN PCs cannot display web pages on the Internet.	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the device is correct, and then you can use the ping utility, discussed on page 76, to test connectivity with your ISP's DNS server.
Web pages	

Problem	Troubleshooting Suggestion
I forgot/lost my user ID or password.	If you have not changed the password from the default, try using "admin" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the rear panel of the device for 5 seconds. Then, type the default User ID and password shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
I cannot access the web pages from my browser.	Use the ping utility, discussed in the following section, to check whether the PC can communicate with the device's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the device*.*
My changes to the web pages are not being retained.	Be sure to use the *Confirm Changes* function after any changes.

Diagnosing Problem using IP Utilities

Ping

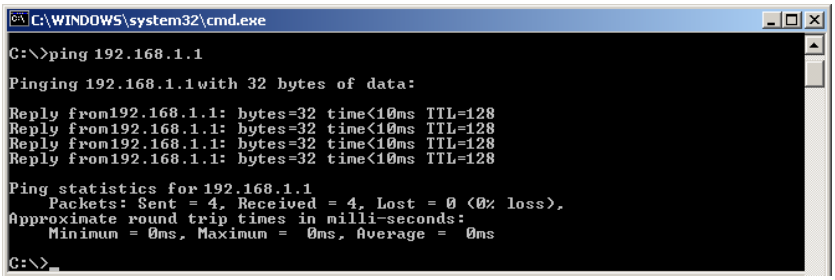
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

ping 192.168.1.1

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window is displayed:



If the target computer cannot be located, you will receive the message Request timed out.

Using the ping command, you can test whether the path to the device is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

nslookup

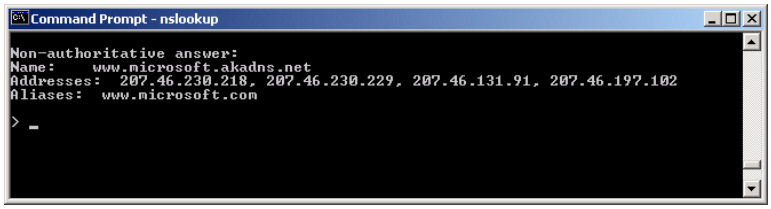
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

Nslookup

Click OK. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown below:



There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type exit and press [Enter] at the command prompt.

14 Appendix E - Advanced DSL port attributes

The following table displays detailed information about the advanced DSL port attributes.

Note

You should only need to refer to these attributes if your ISP has asked you to check something or if you are experienced in DSL port configuration.

Attribute	Value
Line Rate	DSL down stream trained rate (cells/sec)
TxCellTransmitted	Number of transmitted ATM cells
RxCellReceived	Number of received ATM cells
Cbr_CPS	Bit rate for CBR QoS Class
Rvbr SCR_CPS	Sustained cell rate for rt-vbr
Vbr SCR_CPS	Sustained cell rate for nrt-vbr
Rvbr PCR_CPS	Peak cell rate for rt-vbr
Vbr PCR_CPS	Peak cell rate for nrt-vbr
Ubr_CPS	Cell rate for UBR+
Ubr MCR_CPS	Minimum Cell rate for UBR+
CACMode	Gives CAC Mode
CACFunction	Call Admission control function
Port Speed Hook	Function to accommodate the port speed changes
Vpi Range	Range of valid VPI
Vci Range	Range of valid VCI
Default Pcr	Default Peak Cell Rate
Traffic Shaping	Gives weather traffic shaping is enabled/disabled
Ni Type	Network Interface Type
Is Dsl Dma Up	Operational Status of DSL DMA block
Enabled Channels	Number of enabled channels
DSP Firmware Version	DSP code version number
DSP Version	DSL driver version number
Connected	Current connected state: True – modem is connected to a remote modem False – modem is not connected to a remote modem
Operational Mode	Current operating (connected) mode (modulation)

Attribute	Value
State	Current state of the device: Idle – not connected or attempting to connect HandShake – connecting/hunting for remote modem Training – connecting/found a remote modem Showtime – connected to remote modem
Watchdog	Watchdog timer which confirms that the DSP is executing a program correctly
Operation Progress	Detailed startup information to be used for debugging
Last Failed	This value is reset to 0 each time a startup is attempted. If there is a failure, it indicates the reason for the failure.
Tx Bit Rate	Transmit rate (bits per second) of the device
Rx Bit Rate	Receive rate (bits per second) of the device
Tx Cell Rate	Transmit rate (cells per second) of the device
Rx Cell Rate	Receive rate (cells per second) of the device
Phy TXCell Count	Transmit ATM cell counter
Phy RXCell Count	Receive ATM cell counter
Phy Cell Drop Count	UTOPIA cell drop counter
Overall Failure	Indicates the cause of failure
Local ITUCountry Code	Country code used by the device (modulation specific)
Local SEF	Number of severely errored frame defects received by the device
Local End LOS	Number of loss of signal defects received by the device
Local SNRMargin	The local Signal to Noise Ration margin
Local Line Attn	The local attenuation values
Local Tx Power	Current transmit power attenuation of the device
Local Fast Channel Rx Rate	Receive rate (bits per second) of the device on the fast path
Local Fast Channel Tx Rate	Transmit rate (bits per second) of the device on the fast path
Local Fast Channel FEC	Instances of Forward Error Correction required by the device on the fast channel
Local Fast Channel CRC	Number of CRC errors received by the device on the fast channel
Local Fast Channel HEC	Number of ATM Cell Header errors corrected by the device on the fast channel
Local Fast Channel NCD	Number of no cell delineation received by the device on the fast channel
Local Fast Channel OCD	Number of out of cell delineation received by the device on the fast channel
Local Interleaved Channel Rx Rate	Receive rate (bits per second) of the device on the interleaved path
Local Interleaved Channel Tx Rate	Transmit rate (bits per second) of the device on the interleaved path

Attribute	Value
Local Interleaved Channel FEC	Instances of Forward Error Correction required by the device on the interleaved channel
Local Interleaved Channel CRC	Number of CRC errors received by the device on the interleaved channel
Local Interleaved Channel HEC	Number of ATM Cell Header errors corrected by the device on the interleaved channel
Local Interleaved Channel NCD	Number of no cell delineation received by the device on the interleaved channel
Local Interleaved Channel OCD	Number of out of cell delineation received by the device on the interleaved channel
Remote SEF	Number of severely errored frame defects received by the device
Remote LOS	Number of loss of signal defects received by the device
Remote Line Attn	The remote attenuation values
Remote SNRMargin	The remote Signal to Noise Ration margin
Remote Fast Channel FEC	Instances of Forward Error Correction required by the device on the fast channel
Remote Fast Channel CRC	Number of CRC errors received by the device on the fast channel
Remote Fast Channel HEC	Number of ATM Cell Header errors corrected by the device on the fast channel
Remote Fast Channel NCD	Number of no cell delineation received by the device on the fast channel
Remote Interleaved Channel FEC	Instances of Forward Error Correction required by the device on the interleaved channel
Remote Interleaved Channel CRC	Number of CRC errors received by the device on the interleaved channel
Remote Interleaved Channel HEC	Number of ATM Cell Header errors corrected by the device on the interleaved channel
Remote Interleaved Channel NCD	Number of no cell delineation received by the device on the interleaved channel
Activate Line	Abort – deactivates the DSL link None – signifies that this parameter has been read Start – activates the DSL link
Host Control	Disable – terminates any host/API interaction with the DSP (for testing purposes) Enable – enables host/API interaction with the DSP
Auto Start	"True" - A Connection will be established at power up. "False" - The modem will remain in Idle mode at power up.
Failsafe	True – a failsafe timer is activated when a startup request is made. Once a connection has been established, the failsafe timer is disabled False – a failsafe timer is not activated when a startup request is made

Attribute	Value
Whip	Possible Values if compiled for Whip Serial: Serial or Inactive Possible Values if compiled for Whip TCP: TCP or Inactive Possible Values if compiled for Whip Serial/TCP: Serial, TCP or Inactive
Whip Active	Indicated state of whip. Possible values are Inactive, SerialActive and TCPActive
Action	An action given when ActivateLine is set to Start. Possible values are Startup, SpectrumReverb, SpectrumMedely or SpectrumPilot
Standard	Indicates the preferred standard compliance. *Multimode* indicates that the device automatically detects the other end as one of the supported standards.
Utopia Interface	Level1 – Utopia Level 1 internal framing is used with the DSP Level2 – Utopia Level 2 internal framing is used with the DSP
EC FDM Mode	EC – enables Echo Cancellation. This setting is necessary if your device is connected to a high speed CO. FDM – enables Frequency Division Multiplexing
Max Bits Per Bin	The maximum number of bits per bin. This can be any value between 1 and 15
Tx Start Bin	A value that indicates the lowest bin number allowed for transmit signal
Tx End Bin	A value that indicates the highest bin number allowed for transmit signal
Rx Start Bin	A value that indicates the lowest bin number allowed for receive signal
Rx End Bin	A value that indicates the highest bin number allowed for receive signal
Rx Auto Bin Adjust	Disable – the bin settings configured as the RxStartBin/RxEndBin parameters are used Enable – DSP automatically adjusts the bin selection for receive signal
Tx Attenuation	A value between 0dB and 12dB that indicates the transmit power attenuation
Bit Swap	Disable – disables the adjustment of the number of bits assigned to a subcarrier without interrupting data flow Enable – enables the adjustment off the number of bits assigned to a subcarrier without interrupting data flow
Max Down Rate	A value that sets the maximum downstream rate for those applications where it is necessary to limit the downstream data rate
Physical Port	A value between 0 and 14 that sets the Utopia Level 2 Utopia address
Retrain	Disable – disables full retrain capability Enable – enables full retrain capability

Attribute	Value
Detect Noise	Enables/disables noise detection (only valid for Annex AHS)
Capability	This parameter controls whether the CPE will attempt to startup using alternate standards if the CO does not support G.Span (High Speed (HS)). The CPE has the ability to connect in either ADSL Annex A or G.Span. This is provided by the ADSL/Annex A /G.Span Auto Detect feature. The standard used depends on the capability of the CO. Using Auto Detect, startup at the CPE is first attempted in Annex A. The CO is the master and the CPE is the slave. If the result of handshake with the CO is G.Span (HS), then the CPE will switch to G.Span. If the CO does not support G.Span, then the resultant connection will be ADSL Annex A. This parameter must be set to AHS to configure the modem for A & HS 'two-speed' Auto Detect. For Auto Detect, all other parameters should be set to the Annex A profile. If UTOPIA Level 2 framing is set (using the UtopiaInterface parameter), ensure that the UTOPIA address is set (using the PhysicalPort parameter) as there is no default value. If the result of handshake with the CO is G.Span (HS), then the CPE will switch to G.Span and the appropriate CPE parameters will be automatically re-configured by the DSP for G.Span operation. A: Annex A capable AHS: Annex A or High Speed capable Disable: the device does not send any standards capability information to the CO.
Coding Gain	The gain due to trellis/RS coding. Its value ranges from 0-7 dB. *Auto* automatically selects the coding gain.
Framer Type	Value can be set to Type 0 – 3 or Type3ET. To enable DataBoost set FramerType to Type3ET
Dying Gasp	Enables/disables dying gasp.
Defaults	Sets the recommended default parameters for a given Standard.
Reset Defaults	Reset device to use default port configuration

15 Appendix F - Glossary

Term	Description
802.11	A family of specifications for wireless LANs developed by a working group of the IEEE. This inan Ethernet protocol, often called Wi-Fi.
10BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See *data rate, Ethernet*.
100BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See *data rate, Ethernet*.
ADSL	Asymmetric Digital Subscriber Line The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
Analog	An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See *digital*.
ATM	Asynchronous Transfer Mode A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See *data rate*.
Authenticate	To verify a user's identity, such as by prompting for a password.
Binary	The "base two" system of numbers that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See bit, IP address, network mask.
Bit	Short for "binary digit," a bit is a number that can have two values, 0 or 1. See binary.

Bps	bits per second
Bridging	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing which can add more intelligence to data transfers by using network addresses instead. The device can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See routing.
Broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
Broadcast	To send data to all computers on a network.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. See DHCP.
DHCP server	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
Digital	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See analog.
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See domain name.
Domain name	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a

	web site. See DNS.
Download	To transfer data in the downstream direction, i.e., from the Internet to the user.
DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Encryption keys	See network keys
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.
FTP	File Transfer Protocol A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
Gbps	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
Host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See web browser, web site.
Hub	A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE	The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.
Internet	The global collection of interconnected networks used for both private and business communications.

Intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	See TCP/IP.
IP address	Internet Protocol address The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See domain name, network mask.
ISP	Internet Service Provider A company that provides Internet access to its customers, usually for a fee.
LAN	Local Area Network. A network limited to a small geographic area, such as a home or small office.
LED	Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the device are LEDs.
MAC address	Media Access Control address The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; NN:NN:NN:NN:NN:NN.
Mask	See network mask.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
NAT	Network Address Translation A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
Network	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.

Network keys	(Also known as encryption keys.) 64-bit and 128-bit encryption keys used in WEP wireless security schemes. The keys encrypt data over the WLAN, and only wireless PCs configured with WEP keys that correspond to the keys configured on the device can send/receive encrypted data.
Network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See binary, IP address, subnet.
NIC	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See Ethernet, RJ-45.
Packet	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
Ping	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
Port	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
PPP	Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the device uses two forms of PPP called PPPoA and PPPoE. See PPPoA, PPPoE.
PPPoA	Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.
PPPoE	Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
Protocol	A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
Remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.

RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
RJ-11	Registered Jack Standard-11 The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.
RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
Routing	Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See DNS.
Subnet	A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See network mask.
Subnet mask	A mask that defines a subnet. See network mask.
TCP	See TCP/IP.
TCP/IP	Transmission Control Protocol/Internet Protocol The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.
Telnet	An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.
TFTP	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
TKIP	Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and

	sequencing rules and supports re-keying mechanisms.
Triggers	Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them. Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.
Twisted pair	The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See 10BASE-T, 100BASE-T, Ethernet.
Unnumbered interfaces	An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.1.1). The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.
Upstream	The direction of data transmission from the user to the Internet.
VC	Virtual Circuit A connection from your DSL router to your ISP.
VCI	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See VC.
VPI	Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See VC.

WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the device, WAN refers to the Internet.
Web browser	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See HTTP, web site, WWW.
Web page	A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See hyperlink, web site.
Web site	A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See hyperlink, web page.
WEP	Wired Equivalent Privacy (WEP) encrypts data over WLANs. Data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.
Wireless	Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. See wireless LAN.
Wireless LAN	A wireless LAN (WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.
WPA	Wi-Fi Protected Access WPA is an initiative by the IEEE and Wi-Fi Alliance to address the security limitations of WEP. WPA provides a stronger data encryption method (called Temporal Key Integrity Protocol (TKIP)). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device.

	It provides improved data encryption and stronger user authentication. The mode of WPA supported on your device is called Pre-Shared Key (PSK), which allows you to manually enter a type of key called a pass phrase.
WWW	World Wide Web Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.

16 Appendix G - Specification

A1. Hardware Specifications

- LAN Interface
- Four ports 10/100BaseT Ethernet switch HUB, IEEE 802.3/3u compliant with MDI/MDIX auto detection and correction
- Connector – RJ-45
- Integrated 802.11b/g WLAN Access Point

- WAN ADSL Line Interface
- Compliant with ITU-T G.992.1, G.992.2, G.992.3, G.992.5 and ANSI T1.413 Issue 2
- Line Impedance: 100 Ω
- Connection Loops: One (pair wire)
- Connector: RJ-11

- Indicators
- LAN – Green LED indicates LAN data transmitting / receiving
- WLAN– Green LED indicates wireless AP enabled
- Encendido– Green LED indicates power and operation
- ADSL – Green LED indicates ADSL connection
- PPP – Green LED indicates PPPoA or PPPoE connection statues

- OAM&P
- Local: Telnet or Web management via Ethernet
- Remote: Telnet or Web Management

- Environment
- Operation Temperature: 0°C ~ 40°C
- Operation Humidity: 5% ~ 95%
- Storage Temperature: -20 ~ +85°C
- Storage Humidity: 5%~95%

- Power
- AC Adapter: Input 100/240VAC, 50/60Hz; Output 12VDC 1A

- Certificates
- CE, CB

A2. Software Specifications

- ATM
  - ATM Cells over ADSL, AAL5
  - Bridge mode: Supports 8 PVCs
  - Router mode: Supports 5 PVCs
  - Supports UBR, CBR, VBR-nrt, and VBR-rt traffic classes
  - ATM Forum UNI 3.0, UNI 3.1, UNI 4.0
  - ILMI 4.0
  - Payload encapsulations:
    RFC2684 (RFC1483), multi-protocol encapsulation
    RFC2225 (RFC1577), Calssical IP and ARP over ATM
    RFC2364, PPP over ATM
- Bridging
  - Transparent Bridging and spanning tree protocol (IEEE 802.1D)
  - RFC2684 (RFC 1483) Bridged
  - Supports 802.1p/q prioritized tagged VLAN
  - IP and PPPoE packet filtering
  - ZIPB (Zero installation PPP Bridge)
  - Port to PVC binding
- Routing
  - IP routing: RIP v1 and RIP v2, and static routing
  - PPPoE and IP over ATM, PPP over ATM
  - PAP and CHAP for user authentication in PPP connection
  - RFC2684 (RFC1483) Routed
  - NAT/PAT with extensive ALG support
  - DNS relay
  - IP multicasting, IGMP v1/v2 and IGMP proxy
  - Multihoming, IP aliasing and unnumbered IP interfaces
  - Virtual interface and secondary IP addresses
  - Supports IP QoS per RFC2472/2475
- Wireless LAN
  - WEP: 64 or 128 bits key length
  - WPA (Wi-Fi Protected Access) and WPA2 in PSK mode or using the EAP with Radius
  - WME/WMM to support media service
  - Access control list based on MAC address
  - Virtual AP supports multiple BSSID
- Configuration and Network Management Features
  - TR-037 compliant auto-configuration using ILMI
  - SNMP V1, V2, and V3 agent – over IP, EOC and IMLI VCC
  - SNMP MIB II, DSL MIB, AToM MIB and WLAN MIB
  - DHCP client, server and reply for IP management
  - UPnP Internet Gateway Device (IGD v1)
  - System Log capability
  - WEB, SNMP and Telnet for local or remote management
  - TFTP or HTTP for firmware upgrade and configuration

Note: The hardware and software specifications are subjected to change without notices.

17 Appendix I - Regulation

FCC Part 15 Notice

Warning: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 to the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, used, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is unlikely to cause harmful interference. But if it does, the user will be required to correct the interference at his or her own expense. The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless we expressly approves the changes or modifications.

FCC Part 15 Notice with Wireless

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Warning: Operation is subject to the following two conditions:
1) This device may not cause harmful interference.
2) This device must accept any interference received including interference that may cause undesired operation.

FCC Part 68 Notice

This equipment complies with Part 68 of FCC Rules. On the base unit of this equipment is a label that contains, among other information, the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. IF REQUESTED, THIS INFORMATION MUST BE GIVEN TO THE TELEPHONE COMPANY.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in it is facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

NOTICE: The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or an electronic device to send any message via a telephone fax machine, unless such a message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission the following information:

- ✓ The date and time of transmission
- ✓ Identification of either business, business entity or individual sending message
- ✓ Telephone number of either the sending machine, business entity or individual

Warning: Users should not attempt to make such connections themselves, but should contact appropriate electric inspection authority, or electrician, as appropriate.
Do not use any other power adapter except the one that accompanies the unit. Use of other adapter could result in damage to the unit. To prevent electronic shock, please do not open the cover.

UL Safety Regulations

- ✓ Disconnect TNV circuit connector or before removing cover or equivalent.
- ✓ Disconnect TNV circuit connector(s) before disconnecting power.
- ✓ Do not use this product near water for example, near a bathtub, washbowl, and kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- ✓ Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening.
- ✓ Do not use the telephone to report a gas leak in the vicinity of the leak.
- ✓ Use only the power cord batteries indicated in this manual. Do not dispose of batteries in a fire, as they may explode. Check with local codes for possible special disposal instructions.

No. 26 AWG Telephone Line Cord shall either be provided with the equipment or shall be described in the safety instruction. If fuse (F1) is not present, see the caution statement listed below:

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

TELV1.0XA7968081